

504p0878w000

(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関  
国際事務局



(43) 国際公開日  
2001年3月15日 (15.03.2001)

PCT

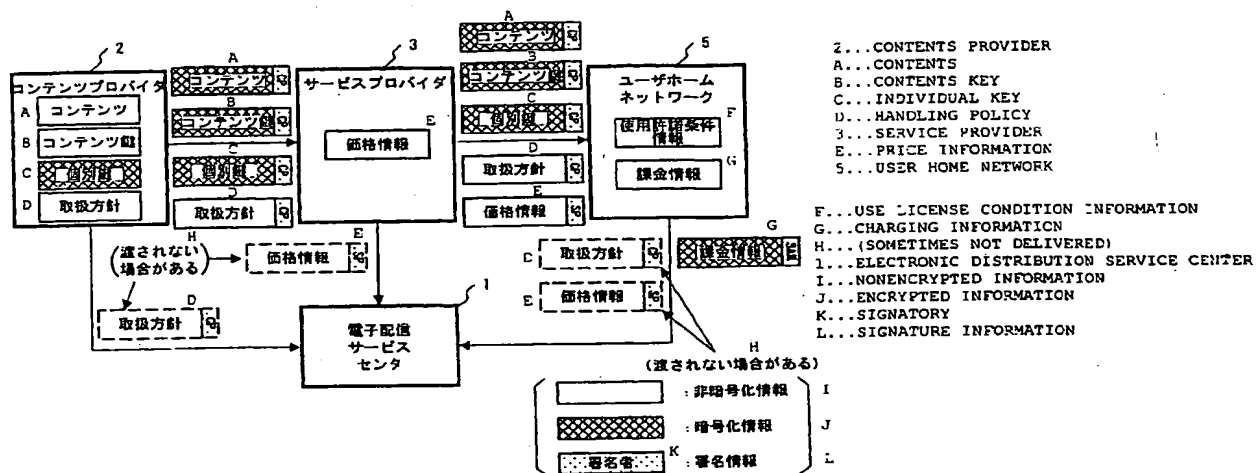
(10) 国際公開番号  
WO 01/19017 A1

- (51) 国際特許分類: H04L 9/32, G06F 15/00, H04N 5/91, G11B 20/10, G10K 15/04, H04N 7/167
- (71) 出願人(米国を除く全ての指定国について): ソニー株式会社 (SONY CORPORATION) [JP/JP]; 〒141-0001 東京都品川区北品川6丁目7番35号 Tokyo (JP).
- (21) 国際出願番号: PCT/JP00/06089
- (72) 発明者; および
- (22) 国際出願日: 2000年9月7日 (07.09.2000)
- (75) 発明者/出願人(米国についてのみ): 石橋義人 (ISHIBASHI, Yoshihito) [JP/JP]. 大石文於 (OHISHI, Tateo) [JP/JP]. 武藤明宏 (MUTO, Akihiro) [JP/JP]. 北原 淳 (KITAHARA, Jun) [JP/JP]. 白井太三 (SHIRAI, Taizou) [JP/JP]; 〒141-0001 東京都品川区北品川6丁目7番35号 ソニー株式会社内 Tokyo (JP).
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (30) 優先権データ:
- |              |                         |    |
|--------------|-------------------------|----|
| 特願平11/253660 | 1999年9月7日 (07.09.1999)  | JP |
| 特願平11/253661 | 1999年9月7日 (07.09.1999)  | JP |
| 特願平11/253662 | 1999年9月7日 (07.09.1999)  | JP |
| 特願平11/253663 | 1999年9月7日 (07.09.1999)  | JP |
| 特願平11/260638 | 1999年9月14日 (14.09.1999) | JP |
| 特願平11/264082 | 1999年9月17日 (17.09.1999) | JP |
| 特願平11/265866 | 1999年9月20日 (20.09.1999) | JP |
- (74) 代理人: 弁理士 田辺恵基 (TANABE, Shigemoto); 〒150-0001 東京都渋谷区神宮前1丁目11番11-508号 グリーンフアンタジアビル5階 Tokyo (JP).
- (81) 指定国(国内): CN, KR, US.
- (84) 指定国(広域): ヨーロッパ特許 (DE, FR, GB).

[続葉有]

(54) Title: CONTENTS MANAGEMENT SYSTEM, DEVICE, METHOD, AND PROGRAM STORAGE MEDIUM

(54) 発明の名称: コンテンツ管理システム、装置、方法及びプログラム格納媒体



(57) Abstract: An information receiving device receives identification information and encrypted identification information and compares them so as to prevent unauthorized use of contents data. Contents data encrypted by a contents key and the contents key are recorded in a data storage device so as to enable another device to reproduce the contents data, thereby enhancing the versatility. A managing device manages the contents data in the data storage device so as to enable another device to use it. An information control device validates the signature of usable data so as to prevent unauthorized use of the contents data. The contents key and its handling policy, and the contents data encrypted by means of the contents key and contents use license condition information are stored in the data storage device so as to provide the contents data safely. An information recording device can select desired contents data and store it in the data storage device. An information receiving device can prevent use of contents data inhibited to provide and specified in a providing inhibition list.

[続葉有]

WO 01/19017 A1



添付公開書類：  
— 国際調査報告書

2文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

---

(57) 要約:

情報受信装置が識別情報と暗号化された識別情報とを受信して比較し、コンテンツデータの不当な利用を防止できる。またデータ格納装置にコンテンツ鍵で暗号化されたコンテンツデータとコンテンツ鍵とを記録して他の機器でもコンテンツデータを再生させて汎用性を向上させ得る。さらに管理装置はデータ格納装置内のコンテンツデータを管理して他の機器にも利用させ得る。さらに情報規制装置は利用可能データの署名を検証してコンテンツデータの不当な利用を防止できる。さらにデータ格納装置にコンテンツ鍵及びその取扱方針とコンテンツ鍵で暗号化したコンテンツデータ及びその使用許諾条件情報とを格納してコンテンツデータを安全に提供できる。さらに情報記録装置は好みのコンテンツデータを選定してデータ格納装置に格納できる。さらに情報受信装置は提供禁止リストで提供禁止対象のコンテンツデータの利用を防止できる。

## コンテンツ管理システム、装置、方法及びプログラム格納媒体

情報送信システム、情報送信装置及び方法、情報受信装置及び方法、記録再生システム、記録再生装置及び方法、再生装置及び方法、データ格納装置及び方法、データ管理システム、管理装置、データ管理方法、データ管理移動方法、情報提供システム、情報規制装置及び方法、データ利用方法、情報提供装置及び方法、情報記録装置、リスト送信装置及び方法、プログラム格納媒体

## 技術分野

本発明は情報送信システム、情報送信装置及び方法、情報受信装置及び方法、記録再生システム、記録再生装置及び方法、再生装置及び方法、データ格納装置及び方法、データ管理システム、管理装置、データ管理方法、データ管理移動方法、情報提供システム、情報規制装置及び方法、データ利用方法、情報提供装置及び方法、情報記録装置、リスト送信装置及び方法、プログラム格納媒体に関し、例えばコンテンツ所有者又は販売者が、コンテンツを安全にコンテンツ利用者に配送し得る情報送信システムに適用して好適なものである。

## 背景技術

従来、音楽などの情報（コンテンツ）を暗号化し、所定の契約を交わしたユーザの情報処理装置に送信し、ユーザがその情報処理装置でコンテンツを復号して、利用するシステムがある。

例えば図116に示すように、2つのコンテンツ送信装置および1つのコンテンツ受信装置が設けられている場合について説明する。

第1のコンテンツ送信装置600は、データ暗号部601、データ暗号部602、コンテンツ鍵生成部603、耐タンパメモリ（Tamper Resistant Memory）604を有している。なお、ここで言う耐タンパメモリとは、第3者に容易にデータを読み出されないものであればよく、特にハード

ウェア的制限は必要ない（例えば、入室管理された部屋の中にあるハードディスクや、パスワード管理されたパソコンのハードディスク等でよい）。耐タンパメモリ 604 にはコンテンツ鍵（Content Key） $K_{co}$  を暗号化するのに必要な配送鍵（Distribution Key） $K_d$  が、予め電子配信サービスセンタ（図示せず）から供給され、保存されている。

第1のコンテンツ送信装置 600 は、コンテンツ受信装置 620 に渡すデータを生成するため、コンテンツ鍵生成部 603 を用いてコンテンツ鍵  $K_{co1}$  を生成し、この鍵を用いてデータ暗号部 601 にてコンテンツを暗号化する。また、コンテンツ鍵  $K_{co1}$  はデータ暗号部 602 にて配送鍵  $K_d$  を用いて暗号化される。これら暗号化されたコンテンツおよびコンテンツ鍵  $K_{co1}$  がコンテンツ受信装置 620 に送信される。

因に、第2のコンテンツ送信装置 610 は、コンテンツ送信装置 600 と同様にして、データ暗号部 611、データ暗号部 612、コンテンツ鍵生成部 613、耐タンパメモリ 614 を有し、コンテンツ鍵生成部 613 においてコンテンツ鍵  $K_{co2}$  を生成し、この鍵を用いてデータ暗号部 611 によりコンテンツを暗号化する。またデータ暗号部 612 は電子配信サービスセンタ（図示せず）から供給される配送鍵  $K_d$  を用いてコンテンツ鍵  $K_{co2}$  を暗号化する。かくして第2のコンテンツ送信装置 610 は、暗号化されたコンテンツ及び暗号化されたコンテンツ鍵  $K_{co2}$  をコンテンツ受信装置 620 に送信する。

コンテンツ受信装置 620 は、送受信部 621、上位コントローラ 622、暗号処理部 623、メモリ 624、データ復号部 625、データ復号部 626、耐タンパメモリ 627 を有する。なお、コンテンツ利用者が不特定多数であり、コンテンツ利用者が機器をどのように扱うか把握できないため、ここで言う耐タンパメモリとはハードウェア的に内部データが保護される必要性があり、従って暗号処理部 623 は、外部からアクセスしにくい構造を持った半導体チップで、多層構造を有し、その内部の耐タンパメモリはアルミニウム層等のダミー層に挟まれ、また、動作する電圧及び又は周波数の幅が狭い等、外部から不正にデータ



の読み出しが難しい特性を有する。そして、耐タンパメモリ 627 には、電子配信サービスセンタ（図示せず）から予め供給された配送鍵  $K_d$  が保存されている。

因に、第1および第2のコンテンツ送信装置 600 および 610 の耐タンパメモリ 604、614 は、外部からアクセス可能なメモリであるが、そのアクセス方法に制約を設けている。それがパスワードであったり、入室管理であったりする。一方、コンテンツ受信装置 620 の耐タンパメモリ 627 においては、メモリそのものが外部から不正にアクセスされない構造を有し、正規のアクセス手段で外部から内部データを読み出す方法も限定されているか、全くない。なお、耐タンパメモリ 627 は外部からその内部データを読み出すことは全くできないが、以前の鍵データ等を用いれば、外部からデータの変更のみできるアクセス方法がある場合がある。また、暗号処理部 623 内では、メモリにアクセスして所定のデータを読み出すことができるのに対して、外部から内部のメモリを読み出すことができないようになされている。

第1または第2のコンテンツ送信者 600 または 610 から送信されてきたコンテンツおよびコンテンツ鍵  $K_{c01}$  及び  $K_{c02}$  は、送受信部 621 で受信され、上位コントローラ 622 に引き渡される。上位コントローラ 622 は、これらのデータをいったんメモリ 624 に保存し、コンテンツを利用する場合には、コンテンツ鍵  $K_{c0}$ 、コンテンツを暗号処理部 623 に引き渡す。これを受信した暗号処理部 623 は、データ復号部 625 で予め耐タンパメモリ 627 に保存しておいた配送鍵  $K_d$  を用いて復号化し、引き続きコンテンツをデータ復号部 626 でコンテンツ鍵  $K_{c0}$  を用いて復号化し、コンテンツを利用する。この時、課金処理を伴う場合がある。

ところで、図 116 に示す情報処理システムにおいては、不当なコンテンツがシステムに提供されたり、又はコンテンツの利用に伴う課金処理により第3者が不当に利益を得るなどのように、当該コンテンツが不当に利用されることを防止するための方法が未だ確立されていない問題があった。

また、かかる情報提供システムにおいては、図 1 1 7 に示す記録再生装置 6 3 0 が設けられる場合があり、かかる記録再生装置 6 3 0 には、例えば、MD (Mini Disk : 商標) でなる記録メディア 6 4 0 が着脱自在に設けられている。

この場合、記録再生装置 6 3 0 は、送受信部 6 3 1、制御部 6 3 2、暗号処理部 6 3 3、伸張部 6 3 4、外部メモリ制御部 6 3 5 を有しており、当該暗号処理部 6 3 3 に予め電子配信サービスセンタ (図示せず) から供給された、コンテンツ鍵  $K_{co}$  を復号化するための配送鍵  $K_d$  を保存していると共に、暗号処理部 6 3 3 固有の保存鍵  $K_{save}$  も保持している。

そして、記録再生装置 6 3 0 は、第 1 または第 2 のコンテンツ送信装置 6 0 0 または 6 1 0 から送信された暗号化されているコンテンツおよびコンテンツ鍵  $K_{co}$  を送受信部 6 3 1 により受信し、当該受信した暗号化されているコンテンツおよびコンテンツ鍵  $K_{co}$  を制御部 6 3 2 に送出する。制御部 6 3 2 は、暗号化されているコンテンツを外部メモリ制御部 6 3 5 を介して記録メディア 6 4 0 に保持し、暗号化されているコンテンツ鍵  $K_{co}$  を暗号処理部 6 3 3 に送出する。

これにより、暗号処理部 6 3 3 は、暗号化されているコンテンツ鍵  $K_{co}$  を配送鍵  $K_d$  を用いて復号化し、引き続きコンテンツ鍵  $K_{co}$  を保存鍵  $K_{save}$  を用いて暗号化し、当該保存鍵  $K_{save}$  で暗号化したコンテンツ鍵  $K_{co}$  を制御部 6 3 2 に送出する。かくして、制御部 6 3 2 は、保存鍵  $K_{save}$  で暗号化したコンテンツ鍵  $K_{co}$  を外部メモリ制御部 6 3 5 を介して記録メディア 6 4 0 に保持させる。

また、記録再生装置 6 3 0 は、コンテンツを利用する場合、制御部 3 2 2 が記録メディア 6 4 0 から暗号化されているコンテンツおよびコンテンツ鍵  $K_{co}$  を読み出し、当該暗号化されているコンテンツを伸張部 6 3 4 に送出すると共に、暗号化されているコンテンツ鍵  $K_{co}$  を暗号処理部 6 3 3 に送出する。これにより暗号処理部 6 3 3 は、暗号化されているコンテンツ鍵  $K_{co}$  を保存鍵  $K_{save}$  で復号化し、得られたコンテンツ鍵  $K_{co}$  を伸張部 6 3 4 を送出する。かくして伸張部 6 3 4 は、コンテンツ鍵  $K_{co}$  を用いて暗号化されているコンテンツを復号化し、これに

よりコンテンツを利用することができる。

ところが、かかる記録再生装置 630 においては、暗号処理部 633 固有の保存鍵  $K_{save}$  で暗号化したコンテンツ鍵  $K_c$  を記録メディア 640 に保持し、当該保存鍵  $K_{save}$  を暗号処理部 633 が保持することにより、記録メディア 630 を例えばコンテンツの記録に用いた記録再生装置 630 以外の他の記録再生装置に装填しても、他の記録再生装置ではコンテンツ鍵  $K_c$  の記録の際に用いた保存鍵  $K_{save}$  を保持していないことにより当該記録メディア 640 に記録されたコンテンツを再生することができない。

従って、かかる記録メディア 640 は、記録再生装置 630 に対して着脱自在に設けられているにも係わらず、その汎用性が著しく低い問題があった。

これに加えて、記録再生装置 630 においては、記録メディアに記録したコンテンツを他の機器や他の記録メディアに記録して利用したいと考えても、当該記録メディアが着脱自在に設けられるために容易には利用し難い問題があった。

さらに、情報処理システムにおいては、コンテンツ受信装置 620 においても、受信したコンテンツが不当に利用されることを防止するための方法が未だ確立されていない問題があった。

さらに、第 1 および第 2 のコンテンツ送信装置 600 および 610 に接続されるコンテンツ受信装置 620 については、ユーザが所有することを前提としているため、当該コンテンツ受信装置 620 を所有していない他の人に対してはコンテンツを容易には提供し難い問題があった。

さらに、情報処理システムにおいては、ユーザがコンテンツ受信装置 620 を用いて好みに応じた複数のコンテンツを所定の記録媒体に記録してアルバム化する場合、コンテンツ受信装置 620 を用いて好みのコンテンツを 1 つづ読み出して記録媒体に記録する必要があり、その記録作業が煩雑な問題があった。

さらに、情報提供システムにおいては、第 1 及び第 2 のコンテンツ送信装置 600 及び 610 から、例えば、欠陥が生じる（データに誤りが生じる）等して送信を中止したコンテンツがコンテンツ受信装置 620 に誤って送信された場合に

は、当該コンテンツ受信装置 620 においてそのコンテンツに対する利用を防止し難い問題があった。

#### 発明の開示

本発明は以上の点を考慮してなされたもので、コンテンツデータが不当に利用されることを防止し得る情報送信システム、情報送信装置、情報受信装置、情報送信方法、情報受信方法及びプログラム格納媒体を提案しようとするものである。

かかる課題を解決するため本発明においては、情報送信装置から所定のコンテンツデータを情報受信装置に送信する情報送信システムにおいて、情報送信装置に、情報受信装置固有の配送鍵で暗号化した、情報送信装置を識別するための識別情報を保持する識別情報保持手段と、配送鍵で暗号化した識別情報と比較するためにコンテンツデータに識別情報を付加する識別情報付加手段と、識別情報を付加したコンテンツデータと共に、配送鍵で暗号化された識別情報を送信する送信手段とを設けるようにし、情報受信装置に、配送鍵を保持する配送鍵保持手段と、識別情報が付加されたコンテンツデータ及び配送鍵で暗号化された識別情報を受信する受信手段と、配送鍵で暗号化された識別情報を当該配送鍵で復号化する復号化手段と、コンテンツデータに付加された識別情報と、復号された識別情報とを比較する比較手段とを設けるようにした。

従って、コンテンツデータに付加された識別情報と、復号された識別情報との比較結果により、コンテンツデータを正当に利用し得るか否かを容易にかつ確実に判断することができ、かくしてコンテンツデータが不当に利用されることを防止し得る情報送信システムを実現することができる。

また、本発明においては、情報受信装置に所定のコンテンツデータを送信する情報送信装置において、情報受信装置固有の所定の配送鍵で暗号化した、情報送信装置を識別するための識別情報を保持する識別情報保持手段と、配送鍵で暗号化された識別情報と比較するためにコンテンツデータに識別情報を付加する識別

情報付加手段と、識別情報を付加したコンテンツデータと共に、配送鍵で暗号化された識別情報を送信する送信手段とを設けるようにした。

従って、コンテンツデータを正当に利用し得るか否かを判断するために比較するコンテンツデータに付加された識別情報と、暗号化された識別情報とを送信対象に提供することができ、かくしてコンテンツデータが不当に利用されることを防止し得る情報送信装置及びプログラム格納媒体を実現することができる。

さらに、本発明においては、情報送信装置から送信された所定のコンテンツデータを受信する情報受信装置において、情報受信装置固有の所定の配送鍵を保持する配送鍵保持手段と、情報送信装置から送信された、情報送信装置を識別するための識別情報が付加されたコンテンツデータと、配送鍵で暗号化された識別情報とを受信する受信手段と、配送鍵で暗号化された識別情報を当該配送鍵で復号化する復号化手段と、コンテンツデータに付加された識別情報と、復号された識別情報とを比較する比較手段とを設けるようにした。

従って、コンテンツデータに付加された識別情報と、復号された識別情報との比較結果により、コンテンツデータを正当に利用し得るか否かを容易にかつ確実に判断することができ、かくしてコンテンツデータが不当に利用されることを防止し得る情報受信装置及び情報受信方法並びにプログラム格納媒体を実現することができる。

さらに、本発明においては、情報送信装置から所定のコンテンツデータを情報受信装置に送信する情報送信システムにおいて、情報送信装置に、コンテンツデータと共に、当該コンテンツデータに対して、予め規定した再送信可能な最大回数データを送信する送信手段を設けるようにし、情報受信装置に、コンテンツデータと共に、最大回数データを受信する受信手段と、最大回数データに基づいて、コンテンツデータの再送信可能な残り回数データを生成する回数データ生成手段と、コンテンツデータと共に、残り回数データを送信する再送信手段とを設けるようにした。

従って、コンテンツデータを予め規定された再送信可能な最大回数よりも多く

再送信することを防止することができ、かくしてコンテンツデータが不当に利用されることを防止し得る情報送信システムを実現することができる。

さらに、本発明においては、所定のコンテンツデータを情報受信装置に送信する情報送信装置において、コンテンツデータと共に、当該コンテンツデータに対して、予め規定した再送信可能な最大回数データを情報受信装置に送信する送信手段を設けるようにした。

従って、コンテンツデータに対して予め規定された再送信可能な最大回数を送信対象に通知することができ、かくしてコンテンツデータが不当に利用されることを防止し得る情報送信装置を実現することができる。

さらに、本発明においては、情報送信装置から送信される所定のコンテンツデータを受信する情報受信装置において、情報送信装置から送信された、コンテンツデータと、当該コンテンツデータに対して予め規定した再送信可能な最大回数データとを受信する受信手段と、最大回数データに基づいて、コンテンツデータの再送信可能な残り回数データを生成する回数データ生成手段と、コンテンツデータと共に、残り回数データを送信する再送信手段とを設けるようにした。

従って、コンテンツデータを予め規定された再送信可能な最大回数よりも多く再送信することを防止することができ、かくしてコンテンツデータが不当に利用されることを防止し得る情報受信装置及び情報受信方法並びにプログラム格納媒体を実現することができる。

さらに、本発明においては、情報送信装置から所定のコンテンツデータを情報受信装置に送信する情報送信方法において、情報送信装置により、コンテンツデータに当該情報送信装置を識別するための識別情報を付加する識別情報付加ステップと、情報送信装置により、識別情報を付加したコンテンツデータと、情報受信装置固有の配送鍵で暗号化した、情報送信装置を識別するための識別情報とを送信する送信ステップと、情報受信装置により、識別情報が付加されたコンテンツデータ及び配送鍵で暗号化された識別情報を受信する受信ステップと、情報受信装置により、配送鍵で暗号化された識別情報を当該配送鍵で復号化する復号化

ステップと、情報受信装置により、コンテンツデータに付加された識別情報と、復号された識別情報とを比較する比較ステップとを設けるようにした。

従って、コンテンツデータに付加された識別情報と、復号された識別情報との比較結果により、コンテンツデータを正当に利用し得るか否かを容易にかつ確実に判断することができ、かくしてコンテンツデータが不当に利用されることを防止し得る情報送信方法を実現することができる。

さらに、本発明においては、情報送信装置から所定のコンテンツデータを情報受信装置に送信する情報送信方法において、情報送信装置により、コンテンツデータと共に、当該コンテンツデータに対して、予め規定した再送信可能な最大回数データを送信する送信ステップと、情報受信装置により、コンテンツデータと共に、最大回数データを受信する受信ステップと、情報受信装置により、最大回数データに基づいて、コンテンツデータの再送信可能な残り回数データを生成する回数データ生成ステップと、情報受信装置により、コンテンツデータと共に、残り回数データを送信する再送信ステップとを設けるようにした。

従って、コンテンツデータを予め規定された再送信可能な最大回数よりも多く再送信することを防止することができ、かくしてコンテンツデータが不当に利用されることを防止し得る情報送信方法及びプログラム格納媒体を実現することができる。

また、本発明は以上の点を考慮してなされたもので、データ格納装置の汎用性を格段的に向上し得る記録再生システム、記録再生装置、再生装置、データ格納装置、記録再生方法、再生方法及びプログラム格納媒体を提案しようとするものである。

かかる課題を解決するため本発明においては、情報送信装置から送信された所定のコンテンツデータを、記録再生装置により着脱自在なデータ格納装置に記録再生する記録再生システムにおいて、情報送信装置に、コンテンツデータを所定のコンテンツ鍵で暗号化するコンテンツ暗号手段と、コンテンツ鍵及び当該コンテンツ鍵で暗号化されたコンテンツデータを送信する送信手段とを設けるように

し、記録再生装置に、情報送信装置から送信されたコンテンツ鍵及び当該コンテンツ鍵で暗号化されたコンテンツデータを受信する受信手段と、受信したコンテンツ鍵及び当該コンテンツ鍵で暗号化されたコンテンツデータをデータ格納装置に送出して記録させ、又は当該データ格納装置からコンテンツ鍵及び当該コンテンツ鍵で暗号化されたコンテンツデータを再生させて読み出す記録再生制御手段とを設けるようにし、データ格納装置に、所定の記録媒体と、所定の保存鍵を保持する保存鍵保持手段と、コンテンツ鍵を保存鍵で暗号化するコンテンツ鍵暗号手段と、保存鍵で暗号化されたコンテンツ鍵及び当該コンテンツ鍵で暗号化されたコンテンツデータを記録媒体に記録し、又は当該記録媒体から保存鍵で暗号化されたコンテンツ鍵及び当該コンテンツ鍵で暗号化されたコンテンツデータを再生する記録再生手段と、保存鍵で暗号化されたコンテンツ鍵を当該保存鍵で復号化するコンテンツ鍵復号手段とを設けるようにした。

従って、記録再生装置側に保存鍵を保持する必要がない分、データ格納装置にコンテンツデータを記録した記録再生装置以外の他の記録再生装置でも当該データ格納装置からコンテンツデータを再生することができ、かくしてデータ格納装置の汎用性を格段的に向上し得る記録再生システムを実現することができる。

また、本発明においては、所定の記録媒体を有するデータ格納装置が着脱自在に設けられた記録再生装置において、所定のコンテンツ鍵で暗号化したコンテンツデータと、当該コンテンツ鍵とをデータ格納装置に送出し、当該データ格納装置固有の所定の保存鍵を用いてコンテンツ鍵を暗号化し、当該保存鍵で暗号化したコンテンツ鍵及び当該コンテンツ鍵で暗号化したコンテンツデータを記録媒体に記録させると共に、当該記録媒体から保存鍵で暗号化したコンテンツ鍵及び当該コンテンツ鍵で暗号化したコンテンツデータを再生させ、保存鍵で暗号化したコンテンツ鍵を当該保存鍵を用いて復号化し、得られた当該コンテンツ鍵及びコンテンツ鍵で暗号化したコンテンツデータをデータ格納装置から読み出す記録再生制御手段を設けるようにした。

従って、保存鍵を保持する必要がない分、他の記録再生装置においてコンテン



ツデータを記録したデータ格納装置から当該コンテンツデータを再生することができ、かくしてデータ格納装置の汎用性を格段的に向上し得る記録再生装置及び記録再生方法並びにプログラム格納媒体を実現することができる。

さらに、本発明においては、所定の記録媒体を有するデータ格納装置が着脱自在に設けられた再生装置において、データ格納装置の記録媒体に予め記録された、所定のコンテンツ鍵で暗号化されたコンテンツデータと、データ格納装置固有の所定の保存鍵で暗号化されたコンテンツ鍵とを再生させ、保存鍵で暗号化されたコンテンツ鍵を当該保存鍵を用いて復号化し、得られた当該コンテンツ鍵及びコンテンツ鍵で暗号化されたコンテンツデータをデータ格納装置から読み出す再生制御手段を設けるようにした。

従って、保存鍵を保持する必要がない分、いずれの再生装置においてもデータ格納装置からコンテンツデータを再生することができ、かくしてデータ格納装置の汎用性を格段的に向上し得る再生装置及び再生方法並びにプログラム格納媒体を実現することができる。

さらに、本発明においては、記録及び又は再生装置に着脱自在に設けられ、当該記録及び又は再生装置の制御のもとに、所定のデータを記録及び又は再生するデータ格納装置において、所定の記録媒体と、所定の保存鍵を保持する保存鍵保持手段と、記録及び又は再生装置との間で、所定のコンテンツ鍵で暗号化した所定のコンテンツデータと、当該コンテンツ鍵とを送受信する通信手段と、記録及び又は再生装置の制御のもとに、コンテンツ鍵を保存鍵で暗号化するコンテンツ鍵暗号手段と、記録及び又は再生装置の制御のもとに、保存鍵で暗号化されたコンテンツ鍵及び当該コンテンツ鍵で暗号化されたコンテンツデータを記録媒体に記録し、又は、当該記録媒体から保存鍵で暗号化されたコンテンツ鍵及び当該コンテンツ鍵で暗号化されたコンテンツデータを再生する記録再生手段と、記録及び又は再生装置の制御のもとに、保存鍵で暗号化されたコンテンツ鍵を当該保存鍵を用いて復号化するコンテンツ鍵復号手段とを設けるようにした。

従って、記録及び再生装置が保存鍵を保持していなくても、コンテンツデータ

を記録及び又は再生させることができ、かくして汎用性を格段的に向上し得るデータ格納装置及びプログラム格納媒体を実現することができる。

さらに、本発明は以上の点を考慮してなされたもので、データ格納装置に記録したコンテンツデータを各種機器で容易に利用し得るデータ管理システム、管理装置、データ格納装置及びデータ管理方法、データ管理移動方法及びプログラム格納媒体を提案しようとするものである。

かかる課題を解決するため本発明においては、データ管理システムにおいて、所定のデータ格納装置と、データ格納装置に所定のコンテンツデータを記録する記録装置と、データ格納装置に格納されたコンテンツデータを取り込み、当該取り込んだコンテンツデータの各種機器への移動をデータ格納装置に代えて管理し、各種機器に接続される管理装置とを設けるようにした。

従って、データ格納装置に記録したコンテンツデータを管理装置の管理の元に、各種機器に容易に移動させることができ、かくしてデータ格納装置に記録したコンテンツデータを各種機器で容易に利用し得るデータ管理システムを実現することができる。

また、本発明においては、各種機器と、所定のデータ格納装置とが接続される管理装置において、データ格納装置に記録された所定のコンテンツデータを取り込み、当該取り込んだコンテンツデータの各種機器への移動をデータ格納装置に代えて管理するようにした。

従って、データ格納装置に記録されたコンテンツデータを当該データ格納装置に代えて管理し、当該コンテンツデータを各種機器に容易に移動させることができ、かくしてデータ格納装置に記録したコンテンツデータを各種機器で容易に利用し得る管理装置及びデータ管理方法並びにプログラム格納媒体を実現することができる。

さらに、本発明においては、所定の記録装置の制御の元に、所定のコンテンツデータを記録するデータ格納装置において、コンテンツデータの各種機器への移動を管理し、当該各種機器が接続される所定の管理装置に接続された際に、当該

管理装置にコンテンツデータを移動するようにした。

従って、記録したコンテンツデータの管理を管理装置に依存し、当該管理装置を介して各種機器に容易に移動させることができ、かくしてデータ格納装置に記録したコンテンツデータを各種機器で容易に利用し得るデータ格納装置及びデータ管理移動方法並びにプログラム格納媒体を実現することができる。

さらに、本発明においては、データ管理方法において、所定の記録装置により、所定のデータ格納装置に所定のコンテンツデータを記録する記録ステップと、各種機器に接続される管理装置により、データ格納装置に格納されたコンテンツデータを取り込み、当該取り込んだコンテンツデータの各種機器への移動をデータ格納装置に代えて管理する管理ステップとを設けるようにした。

従って、データ格納装置に記録したコンテンツデータを管理装置の管理の元に、各種機器に容易に移動させることができ、かくしてデータ格納装置に記録したコンテンツデータを各種機器で容易に利用し得るデータ管理方法を実現することができる。

さらに、本発明は以上の点を考慮してなされたもので、コンテンツデータが不当に利用されることを防止し得る情報提供システム、情報規制装置、情報受信装置、情報提供方法、情報規制方法、データ利用方法及びプログラム格納媒体を提案しようとするものである。

かかる課題を解決するため本発明においては、情報提供システムにおいて、送信される所定のコンテンツデータを受信し、当該受信したコンテンツデータを示す利用許可データに署名を付加して送信する情報受信装置と、利用許可データの署名を検証して、当該利用許可データが不当なデータであるか否かを判断し、当該不当なデータであると判断したときには、情報受信装置に対してコンテンツデータの利用を禁止する情報規制装置とを設けるようにした。

従って、情報規制装置により、情報受信装置によって受信したコンテンツデータが不当に利用されるか否かを未然に判断して、当該コンテンツデータが不当に利用されることを防止し得る情報提供システムを実現することができる。

また、本発明においては、所定の情報受信装置とオンライン接続された情報規制装置において、情報受信装置から、受信した所定のコンテンツデータを示し、かつ署名が付加された利用許可データが送信されることにより、当該利用許可データの署名を検証して、当該利用許可データが不当なデータであるか否かを判断し、当該不当なデータであると判断したときには、情報受信装置に対してコンテンツデータの利用を禁止するようにした。

従って、情報受信装置によって受信したコンテンツデータが不当に利用されるか否かを未然に判断して、当該コンテンツデータが不当に利用されることを防止し得る情報規制装置及び情報規制方法並びにプログラム格納媒体を実現することができる。

さらに、本発明においては、所定の情報規制装置にオンライン接続された情報受信装置において、送信される所定のコンテンツデータを受信し、当該受信したコンテンツデータを示す利用許可データに、当該利用許可データの示すコンテンツデータが他のコンテンツデータに改竄されたか否かを検出し得る署名を付加して情報規制装置に送信するようにした。

従って、情報規制装置に、利用許可データに基づいて、受信したコンテンツデータが不当に利用されるか否かを未然に判断させて、当該コンテンツデータが不当に利用されることを防止し得る情報受信装置及びデータ利用方法並びにプログラム格納媒体を実現することができる。

さらに、本発明においては、情報提供方法において、情報受信装置により、所定のコンテンツデータを受信し、当該受信したコンテンツデータを示す利用許可データに署名を付加して送信する送信ステップと、情報規制装置より、利用許可データの署名を検証して、当該利用許可データが不当なデータであるか否かを判断し、当該不当なデータであると判断したときには、情報受信装置に対してコンテンツデータの利用を禁止する利用禁止ステップとを設けるようにした。

従って、情報規制装置により、情報受信装置によって受信したコンテンツデータが不当に利用されるか否かを未然に判断して、当該コンテンツデータが不当に

利用されることを防止し得る情報提供方法を実現することができる。

さらに、本発明は以上の点を考慮してなされたもので、コンテンツデータを容易に提供し得る情報提供システム、情報提供装置、データ格納装置、情報提供方法、データ格納方法及びプログラム格納媒体を提案しようとするものである。

かかる課題を解決するため本発明においては、情報送信装置から送信される所定のコンテンツデータを情報提供装置に提供する情報提供システムにおいて、情報送信装置に、コンテンツデータを所定のコンテンツ鍵で暗号化する暗号化手段と、コンテンツ鍵及び当該コンテンツ鍵で暗号化されたコンテンツデータを送信する送信手段とを設けるようにし、情報提供装置に、情報送信装置から送信されるコンテンツ鍵及び当該コンテンツ鍵で暗号化されたコンテンツデータを受信する受信手段と、コンテンツ鍵で暗号化されたコンテンツデータを当該コンテンツ鍵で復号化する復号化手段と、コンテンツ鍵で復号化したコンテンツデータに所定の情報を電子透かしにより挿入する電子透かし挿入手段と、当該情報を挿入したコンテンツデータを着脱自在な記録媒体に記録するデータ記録手段とを設けるようにした。

従って、情報利用者がコンテンツデータの受信装置を所有していなくても、情報利用者の記録媒体にコンテンツデータを安全性を確保して記録することができ、かくしてコンテンツデータを容易に提供し得る情報提供システムを実現することができる。

また、本発明においては、情報送信装置から送信された所定のコンテンツデータを提供する情報提供装置において、情報送信装置から送信される所定のコンテンツ鍵で暗号化されたコンテンツデータと、当該コンテンツ鍵とを受信する受信手段と、コンテンツ鍵で暗号化されたコンテンツデータを当該コンテンツ鍵で復号化する復号化手段と、コンテンツ鍵で復号化したコンテンツデータに所定の情報を電子透かしにより挿入する電子透かし挿入手段と、当該情報を挿入したコンテンツデータを着脱自在な記録媒体に記録するデータ記録手段とを設けるようにした。

従って、情報利用者がコンテンツデータの受信装置を所有していなくても、情報利用者の記録媒体にコンテンツデータを安全性を確保して記録することができ、かくしてコンテンツデータを容易に提供し得る情報提供装置及び情報提供方法並びにプログラム格納媒体を実現することができる。

さらに、本発明においては、情報送信装置から送信された所定のコンテンツデータを提供する情報提供装置において、情報送信装置からコンテンツ鍵及び当該コンテンツ鍵で暗号化されたコンテンツデータと共に送信される、コンテンツ鍵の使用条件を規定した取扱方針に基づいて、コンテンツデータの使用条件を規定した使用許諾条件情報を作成する使用許諾条件情報作成手段と、コンテンツ鍵及び当該コンテンツ鍵で暗号化されたコンテンツデータと共に、取扱方針及び使用許諾条件情報を着脱自在な所定のデータ格納装置に送信して格納する格納手段とを設けるようにした。

従って、情報利用者がコンテンツデータの受信装置を所有していなくても、情報利用者のデータ格納装置にコンテンツデータを安全性を確保して記録することができ、かくしてコンテンツデータを容易に提供し得る情報提供装置及び情報提供方法並びにプログラム格納媒体を実現することができる。

さらに、本発明においては、情報提供装置から送信される所定のコンテンツデータを格納するデータ格納装置において、所定の記録媒体と、情報提供装置から送信された、コンテンツ鍵及び当該コンテンツ鍵で暗号化されたコンテンツデータと、コンテンツ鍵の使用条件を規定した取扱方針と、当該取扱方針に基づいて必要に応じて作成されたコンテンツデータの使用条件を規定した使用許諾条件情報とを受信する受信手段と、コンテンツ鍵及び当該コンテンツ鍵で暗号化されたコンテンツデータと、取扱方針及び使用許諾条件情報とを記録媒体に記録する記録手段とを設けるようにした。

従って、情報利用者がコンテンツデータの受信装置を所有していなくても、コンテンツデータを安全性を確保して記録することができ、かくしてコンテンツデータを容易に提供し得るデータ格納装置及びデータ格納装置並びにプログラム格

納媒体を実現することができる。

さらに、本発明は以上の点を考慮してなされたもので、好みに応じた複数のコンテンツデータを容易に記録し得る情報記録装置、データ格納装置、データ格納方法及びプログラム格納媒体を実現するものである。

かかる課題を解決するため本発明においては、所定のコンテンツデータを所定のデータ格納装置に格納する情報記録装置において、複数のコンテンツデータを保持するコンテンツサーバと、当該コンテンツサーバに保持した各コンテンツデータをカテゴリ分けして管理し、所望するカテゴリ及びコンテンツ数が指定されると、当該指定されたカテゴリに属する各コンテンツデータのなかから、指定されたコンテンツ数分の複数のコンテンツデータを任意に選定する選定手段と、選定された各コンテンツデータをコンテンツサーバから読み出してデータ格納装置に格納する格納手段とを設けるようにした。

従って、ユーザの好みに応じた複数のコンテンツデータを容易に選定してデータ格納装置に格納することができ、かくして好みに応じた複数のコンテンツデータを容易に記録し得る情報記録装置及びデータ格納方法並びにプログラム格納媒体を実現することができる。

また、本発明においては、情報記録装置により所定のコンテンツデータが格納されるデータ格納装置において、所定の記録媒体と、情報記録装置から送信された、カテゴリ分けされた複数のコンテンツデータのなかの所望するカテゴリに属し、かつ所望するコンテンツ数分の複数のコンテンツデータを受信するコンテンツ受信手段と、各コンテンツデータを記録媒体に一括して記録する記録手段とを設けるようにした。

従って、情報記録装置から送信される好みに応じた複数のコンテンツデータを記録することができるデータ格納装置及びデータ格納方法並びにプログラム格納媒体を実現することができる。

さらに、本発明は以上の点を考慮してなされたもので、提供禁止対象のコンテンツデータが利用されることをほぼ確実に防止し得る情報提供システム、リスト

送信装置、情報受信装置、情報提供方法、情報受信方法、リスト送信方法及びプログラム格納媒体を提案しようとするものである。

かかる課題を解決するため本発明においては、情報提供システムにおいて、所定のコンテンツデータを送信する情報送信装置と、提供禁止対象に指定されたコンテンツデータを示す提供禁止リストを作成し、当該作成した提供禁止リストを送信するリスト送信装置と、提供禁止リストに基づいて、情報送信装置から送信されるコンテンツデータが提供禁止対象であるか否かを判別し、当該コンテンツデータが提供禁止対象である場合には、当該コンテンツデータの取り込みを中止する情報受信装置とを設けるようにした。

従って、情報受信装置において、提供禁止対象のコンテンツや、利用禁止対象の情報送信装置から送信されたコンテンツを購入することをほぼ確実に防止することができ、かくして提供禁止対象のコンテンツデータが利用されることをほぼ確実に防止し得る情報提供システムを実現することができる。

また、本発明においては、情報送信装置から送信される所定のコンテンツデータを受信する情報受信装置に所定のリストを送信するリスト送信装置において、提供禁止対象に指定されたコンテンツデータを示す提供禁止リストを作成するリスト作成手段と、提供禁止リストを情報受信装置に送信する送信手段とを設けるようにした。

従って、情報受信装置において、提供禁止リストに基づいて、提供禁止対象のコンテンツや、利用禁止対象の情報送信装置から送信されたコンテンツが購入されることをほぼ確実に防止させることができ、かくして提供禁止対象のコンテンツデータが利用されることをほぼ確実に防止し得るリスト送信装置及びリスト送信方法並びにプログラム格納媒体を実現することができる。

さらに、本発明においては、情報送信装置から送信される所定のコンテンツデータと、リスト送信装置から送信される所定のリストを受信する情報受信装置において、リスト送信装置から送信される提供禁止対象に指定されたコンテンツデータを示す提供禁止リストを保持するリスト保持手段と、提供禁止リストに基づ



いて、情報送信装置から送信されるコンテンツデータが提供禁止対象であるか否かを判別し、当該コンテンツデータが提供禁止対象である場合には、そのコンテンツデータの取り込みを中止する取込み中止処理手段とを設けるようにした。

従って、提供禁止対象のコンテンツや、利用禁止対象の情報送信装置から送信されたコンテンツを購入することをほぼ確実に防止することができ、かくして提供禁止対象のコンテンツデータが利用されることをほぼ確実に防止し得る情報受信装置及び情報受信方法並びにプログラム格納媒体を実現することができる。

さらに、本発明においては、情報提供方法において、リスト送信装置により、提供禁止対象に指定されたコンテンツデータを示す提供禁止リストを作成し、当該作成した提供禁止リストを送信するリスト送信ステップと、情報送信装置により、所定のコンテンツデータを送信するデータ送信ステップと、情報受信装置により、提供禁止リストに基づいて、情報送信装置から送信されるコンテンツデータが提供禁止対象であるか否かを判別し、当該コンテンツデータが提供禁止対象である場合には、当該コンテンツデータの取り込みを中止する取込み中止ステップとを設けるようにした。

従って、情報受信装置において、提供禁止対象のコンテンツや、利用禁止対象の情報送信装置から送信されたコンテンツを購入することをほぼ確実に防止することができ、かくして提供禁止対象のコンテンツデータが利用されることをほぼ確実に防止し得る情報提供方法を実現することができる。

因みに、情報受信装置のオンライン機器及びオフライン機器では、当該オンライン機器及びオフライン機器間でコンテンツデータを送信するときに、そのコンテンツデータの識別情報及び送信元の機器の識別情報により履歴情報を作成し、提供禁止リストを受信したときに、履歴情報内を検索し、新たに提供禁止対象となったコンテンツデータが送信されていると、当該コンテンツデータの送信元に自分の保持する最新の提供禁止リストを送信するようにしたことにより、送信元の機器から不正なコンテンツデータが他の機器に拡散することを未然に防止することができる。

## 図面の簡単な説明

図 1 は、本発明による電子音楽配信システムの全体構成を示すブロック図である。

図 2 は、電子配信サービスセンタの構成を示すブロック図である。

図 3 は、鍵の定期的な更新例を示す略線図である。

図 4 は、鍵の定期的な更新例を示す略線図である。

図 5 は、鍵の定期的な更新例を示す略線図である。

図 6 は、鍵の定期的な更新例を示す略線図である。

図 7 は、ユーザ登録データベースのデータ内容を示す略線図である。

図 8 は、グループごとの登録情報を示す略線図である。

図 9 は、コンテンツプロバイダの構成を示すブロック図である。

図 10 は、署名生成処理手順を示すフローチャートである。

図 11 は、署名検証処理手順を示すフローチャートである。

図 12 は、楕円曲線暗号化方法を示すフローチャートである。

図 13 は、楕円曲線暗号化の復号化処理を示すフローチャートである。

図 14 は、サービスプロバイダの構成を示すブロック図である。

図 15 は、ユーザホームネットワークの構成を示すブロック図である。

図 16 は、外部メモリ制御部の動作の説明に供する略線図である。

図 17 は、電子配信専用記録メディアの構成を示すブロック図である。

図 18 は、各機器の持つデータ内容を示すブロック図である。

図 19 は、記録メディアが保持するデータ内容を示すブロック図である。

図 20 は、システム全体のデータの流れを示す略線的ブロック図である。

図 21 は、公開鍵証明書の流れを示す略線的ブロック図である。

図 22 は、コンテンツプロバイダセキュアコンテナを示す略線図である。

図 23 は、コンテンツプロバイダセキュアコンテナを示す略線図である。

図 24 は、コンテンツプロバイダセキュアコンテナを示す略線図である。

図 25 は、コンテンツプロバイダセキュアコンテナを示す略線図である。

- 図 2 6 は、コンテンツプロバイダの公開鍵証明書を示す略線図である。
- 図 2 7 は、コンテンツプロバイダの公開鍵証明書を示す略線図である。
- 図 2 8 は、コンテンツプロバイダの公開鍵証明書を示す略線図である。
- 図 2 9 は、サービスプロバイダセキュアコンテナを示す略線図である。
- 図 3 0 は、サービスプロバイダセキュアコンテナを示す略線図である。
- 図 3 1 は、サービスプロバイダの公開鍵証明書を示す略線図である。
- 図 3 2 は、ユーザ機器の公開鍵証明書を示す略線図である。
- 図 3 3 は、シングルコンテンツの取扱方針を示す図表である。
- 図 3 4 は、アルバムコンテンツの取扱方針を示す図表である。
- 図 3 5 は、シングルコンテンツの取扱方針の他の例を示す図表である。
- 図 3 6 は、アルバムコンテンツの取扱方針の他の例を示す図表である。
- 図 3 7 は、シングルコンテンツの価格情報を示す図表である。
- 図 3 8 は、アルバムコンテンツの価格情報を示す図表である。
- 図 3 9 は、シングルコンテンツの価格情報の他の例を示す図表である。
- 図 4 0 は、アルバムコンテンツの価格情報の他の例を示す図表である。
- 図 4 1 は、使用許諾条件情報を示す図表である。
- 図 4 2 は、課金情報を示す図表である。
- 図 4 3 は、課金情報の他の例を示す図表である。
- 図 4 4 は、利用権内容の一覧を示す図表である。
- 図 4 5 は、利用権を示す図表である。
- 図 4 6 は、シングルコンテンツを示す図表である。
- 図 4 7 は、アルバムコンテンツを示す図表である。
- 図 4 8 は、シングルコンテンツ用の鍵データを示す図表である。
- 図 4 9 は、個別鍵の暗号化処理の説明に供するブロック図である。
- 図 5 0 は、アルバムコンテンツ用の鍵データを示す図表である。
- 図 5 1 は、対称鍵技術を用いた相互認証処理を示すタイミングチャートである。

図 5 2 は、非対称鍵暗号技術を用いた相互認証処理を示すタイミングチャートである。

図 5 3 は、課金情報の送信動作を示す略線的ブロック図である。

図 5 4 は、利益分配処理動作を示す略線的ブロック図である。

図 5 5 は、コンテンツ利用実績の送信動作を示す略線的ブロック図である。

図 5 6 は、コンテンツの配布及び再生処理手順を示すフローチャートである。

図 5 7 は、コンテンツプロバイダへの送信処理手順を示すフローチャートである。

図 5 8 は、決済情報の登録処理手順を示すフローチャートである。

図 5 9 は、機器 I D の新規登録処理手順を示すフローチャートである。

図 6 0 は、機器の追加登録処理手順を示すフローチャートである。

図 6 1 は、登録情報の変更開始条件の判断処理手順を示すフローチャートである。

図 6 2 は、登録情報更新処理手順を示すフローチャートである。

図 6 3 は、据置機器による登録情報更新代理処理手順を示すフローチャートである。

図 6 4 は、据置機器による登録情報更新代理処理手順を示すフローチャートである。

図 6 5 は、セキュアコンテナの送信処理手順を示すフローチャートである。

図 6 6 は、セキュアコンテナの送信処理手順を示すフローチャートである。

図 6 7 は、ホームサーバの購入処理手順を示すフローチャートである。

図 6 8 は、データ読み出し時の改ざんチェック処理手順を示すフローチャートである。

図 6 9 は、データ書込み時の改ざんチェック処理手順を示すフローチャートである。

図 7 0 は、データ書換え時の改竄チェック処理手順を示すフローチャートである。

図 7 1 は、データ削除時の改竄チェック処理手順を示すフローチャートである。

図 7 2 は、ホームサーバによるコンテンツの再生処理手順を示すフローチャートである。

図 7 3 は、ホームサーバによるコンテンツの再生処理手順を示すフローチャートである。

図 7 4 は、ホームサーバによるコンテンツ利用権の代理購入処理手順を示すフローチャートである。

図 7 5 は、購入済利用者の内容変更処理手順を示すフローチャートである。

図 7 6 は、取扱方針のルール部の内容を示す略線図である。

図 7 7 は、価格情報のルール部の内容を示す略線図である。

図 7 8 は、権利内容の変更例を示す略線図である。

図 7 9 は、コンテンツ利用権の再配布処理手順を示すフローチャートである。

図 8 0 は、据置機器でのコンテンツ利用権購入処理手順を示すフローチャートである。

図 8 1 は、使用許諾条件情報のルール部の変遷を示す略線図である。

図 8 2 は、管理移動権の移動処理手順を示すフローチャートである。

図 8 3 は、管理移動権の返還処理手順を示すフローチャートである。

図 8 4 は、本発明による情報送信システムを示すブロック図である。

図 8 5 は、本発明による情報送信システムを示すブロック図である。

図 8 6 は、遠隔再生処理手順を示すフローチャートである。

図 8 7 は、予約購入処理手順を示すフローチャートである。

図 8 8 は、予約購入後の本購入処理手順を示すフローチャートである。

図 8 9 は、ホームサーバが課金する場合の代理購入処理手順を示すフローチャートである。

図 9 0 は、グループ外機器が課金する場合の代理購入処理手順を示すフローチャートである。

図 9 1 は、管理移動権の移動処理の世代管理の説明に供する概念図である。

図 9 2 は、記録再生装置の構成を示すブロック図である。

図 9 3 は、記録再生装置の購入処理手順を示すフローチャートである。

図 9 4 は、記録再生装置の再生処理手順を示すフローチャートである。

図 9 5 は、課金情報の代理処理及び権利の移動処理手順を示すフローチャートである。

図 9 6 は、電子音楽配信システム全体のデータの流れを示すブロック図である。

図 9 7 は、オンライン課金購入処理手順を示すフローチャートである。

図 9 8 は、電子音楽配信システムの構成を示すブロック図である。

図 9 9 は、ホスティングサーバの構成を示すブロック図である。

図 1 0 0 は、K I O S K 端末の構成を示すブロック図である。

図 1 0 1 は、データの流れを示す略線図である。

図 1 0 2 は、K I O S K 端末の購入処理手順を示すフローチャートである。

図 1 0 3 は、K I O S K 端末の購入処理手順を示すフローチャートである。

図 1 0 4 は、K I O S K 端末の購入処理手順を示すフローチャートである。

図 1 0 5 は、K I O S K 端末の購入処理手順を示すフローチャートである。

図 1 0 6 は、K I O S K 端末の購入処理手順の他の例を示すフローチャートである。

図 1 0 7 は、K I O S K 端末の購入処理手順の他の例を示すフローチャートである。

図 1 0 8 は、コンテンツの購入禁止リストを示す図表である。

図 1 0 9 は、コンテンツの再配布／再購入リストを示す図表である。

図 1 1 0 は、コンテンツの再配布／再購入処理手順を示すフローチャートである。

図 1 1 1 は、電子音楽配信システムの他の構成を示すブロック図である。

図 1 1 2 は、パーソナルコンピュータ構成の電子配信サービスセンターの構成

を示すブロック図である。

図 1 1 3 は、パーソナルコンピュータ構成のコンテンツプロバイダの構成を示すブロック図である。

図 1 1 4 は、パーソナルコンピュータ構成のサービスプロバイダの構成を示すブロック図である。

図 1 1 5 は、パーソナルコンピュータを用いたユーザホームネットワークの構成を示すブロック図である。

図 1 1 6 は、従来例を示すブロック図である。

図 1 1 7 は、従来の記録再生装置の構成を示すブロック図である。

発明を実施するための最良の形態

以下、図面について本発明の一実施の形態を詳述する。

#### (1) 情報配信システム

図 1 は、本発明を適用した EMD (Electronic Music Distribution: 電子音楽配信) システム 10 を説明する図である。このシステムでユーザに配信されるコンテンツ (Content) とは、情報そのものが価値を有するデジタルデータで、この例の場合、1つのコンテンツは、1曲分の音楽データに相当する。コンテンツは、1つのコンテンツが1つの単位 (シングル) として、または複数のコンテンツが1つの単位 (アルバム) としてユーザに提供される。ユーザは、コンテンツを購入し (実際には、コンテンツ鍵  $K_c$  を利用する権利を購入し)、提供されるコンテンツを利用する (実際には、コンテンツ鍵  $K_c$  を用いてコンテンツを復号化し、利用する)。なお、勿論、音楽データだけでなく、映像、ゲームプログラム等、コンテンツの販売全てに適用可能である。

電子配信サービスセンタ (END Service Center) 1 は、コンテンツプロバイダ (Content Provider) 2 に個別鍵  $K_i$ 、コンテンツプロバイダ 2 の公開鍵証明書を送信し、サービスプロバイダ (Serv

ice Provider) 3にサービスプロバイダ3の公開鍵証明書を送信し、ユーザホームネットワーク5に対しては配送鍵 $K_d$ や登録情報を送信し、ユーザホームネットワーク5から、コンテンツの利用に応じた課金情報等や登録情報を受信し、課金情報に基づいて利用料金を精算し、コンテンツプロバイダ2、サービスプロバイダ3および電子配信サービスセンタ1自身へ利益分配の処理を行う。

コンテンツプロバイダ2は、デジタル化されたコンテンツを有し、自己のコンテンツであることを証明するために電子透かし（ウォーターマーク（Watermark））をコンテンツに挿入し、コンテンツを圧縮し、および暗号化し、コンテンツの取扱方針を生成し、署名データを付加してサービスプロバイダ3へ送信する。

サービスプロバイダ3は、専用のケーブルネットワーク、インターネット、または衛星通信などから構成されるネットワーク4を介して、コンテンツプロバイダ2から供給されたコンテンツに価格情報を追加し、署名データを付加して、ユーザホームネットワーク5に送信する。

ユーザホームネットワーク5は、サービスプロバイダ3から価格情報を付して送付されたコンテンツを入手し、コンテンツ利用権を購入し、購入処理を実行する。購入した利用権は、例えば再生利用権であったり、コピーする権利であったりする。そして、購入処理により生成された課金情報は、ユーザの保持する機器の、暗号処理部内の耐タンパメモリに保存され、ユーザホームネットワーク5が配送鍵 $K_d$ を電子配信サービスセンタ1から入手する際に、電子配信サービスセンタ1に送信される。

図2は、電子配信サービスセンタ1の機能の構成を示すブロック図である。サービスプロバイダ管理部11は、サービスプロバイダ3にサービスプロバイダ3の公開鍵証明書及び利益分配の情報を供給すると共に、必要に応じてコンテンツに付される情報（価格情報）を受信する。コンテンツプロバイダ管理部12は、コンテンツプロバイダ2に個別鍵 $K_i$ 、配送鍵 $K_d$ で暗号化した個別鍵 $K_i$ および



コンテンツプロバイダ 2 の公開鍵証明書を送信すると共に、利益分配の情報を供給し、必要に応じてコンテンツに付される情報（取扱方針）を受信する。著作権管理部 13 は、ユーザホームネットワーク 5 のコンテンツ利用の実績を示す情報を、著作権を管理する団体、例えば、JASRAC (Japanese Society for Rights of Authors, Composers and Publishers: 日本音楽著作権協会) に送信する。鍵サーバ 14 は、システム全てに使用する鍵の生成、保持、管理を行っており、例えば、コンテンツプロバイダ毎に異なる個別鍵  $K_i$  が生成されるとともに、配送鍵  $K_d$  で暗号化された個別鍵  $K_i$  も併せて生成され、これらはコンテンツプロバイダ管理部 12 を介してコンテンツプロバイダ 2 に供給され、さらに配送鍵  $K_d$  で暗号化された個別鍵  $K_i$  も必要に応じて認証局 22 に供給され、配送鍵  $K_d$  はユーザ管理部 18 を介してユーザホームネットワーク 5 に供給される。また、電子配信サービスセンタ 1 の公開鍵・秘密鍵、ユーザの保持する機器に固有の公開鍵・秘密鍵も全て生成、管理され、公開鍵は認証局 22 に送信され、公開鍵証明書作成に利用される。また、後述する暗号処理部 92 に固有の機器別 ID に応じた保存鍵  $K_{save}$  を生成、保持する場合もある。

電子配信サービスセンタ 1 からコンテンツプロバイダ 2 およびユーザホームネットワーク 5 を構成するホームサーバ 51（後述する）への、鍵の定期的な送信の例について、図 3 乃至図 6 を参照に説明する。図 3 は、コンテンツプロバイダ 2 がコンテンツの提供を開始し、ユーザホームネットワーク 5 を構成するホームサーバ 51 がコンテンツの利用を開始する、2000 年 1 月における、電子配信サービスセンタ 1 が有する配送鍵  $K_d$ 、個別鍵  $K_i$ 、コンテンツプロバイダ 2 が有する個別鍵  $K_i$ 、およびホームサーバ 51 が有する配送鍵  $K_d$  を示す図である。なお、以下省略するが、コンテンツプロバイダ 2 は、個別鍵  $K_i$  に対応する、配送鍵  $K_d$  で暗号化された個別鍵  $K_i$  も保持しているものとする。

図 3 の例において、配送鍵  $K_d$ 、個別鍵  $K_i$  は、暦の月の初日から月の末日まで、使用可能であり、例えば、所定のビット数の乱数である” a a a a a a a a

”の値を有するバージョン1である配送鍵 $K_d$ 、”zzzzzzzz”の値を有するバージョン1である個別鍵 $K_i$ は、2000年1月1日から2000年1月31日まで使用可能（すなわち、2000年1月1日から2000年1月31日の期間にサービスプロバイダ3がユーザホームネットワーク5に配布するコンテンツを暗号化するコンテンツ鍵 $K_c$ は、バージョン1である個別鍵 $K_i$ 暗号化され、バージョン1である個別鍵 $K_i$ は、バージョン1である配送鍵 $K_d$ で暗号化されている）であり、所定のビット数の乱数である”bbbbbbbb”の値を有するバージョン2である配送鍵 $K_d$ 、”yyyyyyyy”の値を有するバージョン2である個別鍵 $K_i$ は、2000年2月1日から2000年2月29日まで使用可能（すなわち、その期間にサービスプロバイダ3がユーザホームネットワーク5に配布するコンテンツを暗号化するコンテンツ鍵 $K_c$ は、バージョン2である個別鍵 $K_i$ で暗号化され、バージョン2である個別鍵 $K_i$ は、バージョン2である配送鍵 $K_d$ で暗号化されている）である。同様に、バージョン3である配送鍵 $K_d$ 、個別鍵 $K_i$ は2000年3月中に使用可能であり、バージョン4である配送鍵 $K_d$ 、個別鍵 $K_i$ は2000年4月中に使用可能であり、バージョン5である配送鍵 $K_d$ 、個別鍵 $K_i$ は2000年5月中に使用可能であり、バージョン6である配送鍵 $K_d$ 、個別鍵 $K_i$ は2000年6月中に使用可能である。

コンテンツプロバイダ2がコンテンツの提供を開始するのに先立ち、電子配信サービスセンタ1は、コンテンツプロバイダ2に、2000年1月から6月まで利用可能な、バージョン1乃至バージョン6の6つの個別鍵 $K_i$ と、それぞれを同一バージョンの配送鍵 $K_d$ で暗号化したものを送信し、コンテンツプロバイダ2は、6つの個別鍵 $K_i$ および配送鍵 $K_d$ で暗号化された個別鍵 $K_i$ を受信し、記憶する。6月分の個別鍵 $K_i$ および配送鍵 $K_d$ で暗号化された個別鍵 $K_i$ を記憶するのは、コンテンツプロバイダ2は、コンテンツを提供する前のコンテンツおよびコンテンツ鍵 $K_c$ の暗号化などの準備に、所定の期間が必要だからである。

また、ホームサーバ51がコンテンツの利用を開始するのに先立ち、電子配信サービスセンタ1は、ホームサーバ51に2000年1月から2000年3月ま

で、利用可能なバージョン1乃至バージョン3である3つの配送鍵 $K_d$ を送信し、ホームサーバ51は、3つの配送鍵 $K_d$ を受信し、記憶する。3月分の配送鍵 $K_d$ を記憶するのは、ホームサーバ51が、回線の混雑等を原因として、電子配信サービスセンタ1に接続できないなどのトラブルにより、コンテンツの購入が可能な契約期間にもかかわらずコンテンツが購入できない等の事態を避けるためであり、また、電子配信サービスセンタ1への接続の頻度を低くしたり、個々の機器の電子配信サービスセンタ1への同時アクセスを押さえ、電子配信サービスセンタ1の負荷を低減するためである。

2000年1月1日から2000年1月31日の期間には、バージョン1である配送鍵 $K_d$ および個別鍵 $K_i$ が、電子配信サービスセンタ1、コンテンツプロバイダ2、ユーザホームネットワーク5を構成するホームサーバ51で利用される。

2000年2月1における、電子配信サービスセンタ1の配送鍵 $K_d$ および個別鍵 $K_i$ のコンテンツプロバイダ2、およびホームサーバ51への送信を図4で説明する。電子配信サービスセンタ1は、コンテンツプロバイダ2に、2000年2月から2000年7月まで利用可能な、バージョン2乃至バージョン7の6つの個別鍵 $K_i$ と、それぞれを同一バージョンの配送鍵 $K_d$ で暗号化したものを送信し、コンテンツプロバイダ2は、6つの個別鍵 $K_i$ および配送鍵 $K_d$ で暗号化された個別鍵 $K_i$ を受信し、受信前に記憶していた個別鍵 $K_i$ および配送鍵 $K_d$ で暗号化された個別鍵 $K_i$ に上書きし、新たな個別鍵 $K_i$ および配送鍵 $K_d$ で暗号化された個別鍵 $K_i$ を記憶する。電子配信サービスセンタ1は、ホームサーバ51に2000年2月から2000年4月まで、利用可能なバージョン2乃至バージョン4である3つの配送鍵 $K_d$ を送信し、ホームサーバ51は、3つの配送鍵 $K_d$ を受信し、受信前に記憶していた配送鍵 $K_d$ に上書きし、新たな配送鍵 $K_d$ を記憶する。電子配信サービスセンタ1は、バージョン1～7である配送鍵 $K_d$ および個別鍵 $K_i$ をそのまま記憶する。これは、不測のトラブルが発生したとき、若しくは不正が発生し、または発見されたときに、過去に利用した配送鍵 $K_d$ を

利用できるようにするためである。

2000年2月1日から2000年2月29日の期間には、バージョン2である配送鍵 $K_d$ および個別鍵 $K_i$ が、電子配信サービスセンタ1、コンテンツプロバイダ2、ユーザホームネットワーク5を構成するホームサーバ51で利用される。

2000年3月1における、電子配信サービスセンタ1の配送鍵 $K_d$ および個別鍵 $K_i$ のコンテンツプロバイダ2、およびホームサーバ51への送信を図5で説明する。電子配信サービスセンタ1は、コンテンツプロバイダ2に、2000年3月から2000年8月まで利用可能な、バージョン3乃至バージョン8の6つの個別鍵 $K_i$ と、それぞれを同一バージョンの配送鍵 $K_d$ で暗号化したものを送信し、コンテンツプロバイダ2は、6つの個別鍵 $K_i$ および配送鍵 $K_d$ で暗号化された個別鍵 $K_i$ を受信し、受信前に記憶していた個別鍵 $K_i$ および配送鍵 $K_d$ で暗号化された個別鍵 $K_i$ に上書きし、新たな個別鍵 $K_i$ および配送鍵 $K_d$ で暗号化された個別鍵 $K_i$ を記憶する。電子配信サービスセンタ1は、ホームサーバ51に2000年3月から2000年5月まで、利用可能なバージョン3乃至バージョン5である3つの配送鍵 $K_d$ を送信し、ホームサーバ51は、3つの配送鍵 $K_d$ を受信し、受信前に記憶していた配送鍵 $K_d$ に上書きし、新たな配送鍵 $K_d$ を記憶する。電子配信サービスセンタ1は、バージョン1～8である配送鍵 $K_d$ および個別鍵 $K_i$ をそのまま記憶する。これは、不測のトラブルが発生したとき、若しくは不正が発生し、または発見されたときに、過去に利用した配送鍵 $K_d$ を利用できるようにするためである。

2000年3月1日から2000年3月31日の期間には、バージョン3である配送鍵 $K_d$ および個別鍵 $K_i$ が、電子配信サービスセンタ1、コンテンツプロバイダ2、ユーザホームネットワーク5を構成するホームサーバ51で利用される。

2000年4月1における、電子配信サービスセンタ1の配送鍵 $K_d$ および個別鍵 $K_i$ のコンテンツプロバイダ2、およびホームサーバ51への送信を図6で

説明する。電子配信サービスセンタ 1 は、コンテンツプロバイダ 2 に、2000 年 4 月から 2000 年 9 月まで利用可能な、バージョン 4 乃至バージョン 9 の 6 つの個別鍵  $K_i$  と、それぞれを同一バージョンの配送鍵  $K_d$  で暗号化したものを送信し、コンテンツプロバイダ 2 は、6 つの個別鍵  $K_i$  および配送鍵  $K_d$  で暗号化された個別鍵  $K_i$  を受信し、受信前に記憶していた個別鍵  $K_i$  および配送鍵  $K_d$  で暗号化された個別鍵  $K_i$  に上書きし、新たな個別鍵  $K_i$  および配送鍵  $K_d$  で暗号化された個別鍵  $K_i$  を記憶する。電子配信サービスセンタ 1 は、ホームサーバ 51 に 2000 年 4 月から 2000 年 6 月まで利用可能な、バージョン 4 乃至バージョン 6 である 3 つの配送鍵  $K_d$  を送信し、ホームサーバ 51 は、3 つの配送鍵  $K_d$  を受信し、受信前に記憶していた配送鍵  $K_d$  に上書きし、新たな配送鍵  $K_d$  を記憶する。電子配信サービスセンタ 1 は、バージョン 1 ～ 9 である配送鍵  $K_d$  および個別鍵  $K_i$  をそのまま記憶する。これは、不測のトラブルが発生したとき、若しくは不正が発生し、または発見されたときに、過去に利用した配送鍵  $K_d$  を利用できるようにするためである。

2000 年 4 月 1 日から 2000 年 4 月 30 日の期間には、バージョン 4 である配送鍵  $K_d$  および個別鍵  $K_i$  が、電子配信サービスセンタ 1、コンテンツプロバイダ 2、ユーザホームネットワーク 5 を構成するホームサーバ 51 で利用される。

このように、あらかじめ先の月の配送鍵  $K_d$  および個別鍵  $K_i$  を配布しておくことで、仮にユーザが 1、2 ヶ月全くセンタにアクセスしていなくても、一応、コンテンツの買い取りが行え、時を見計らって、センタにアクセスすることにより鍵を受信することができる。

電子配信サービスセンタ 1 の経歴データ管理部 15 (図 2) は、ユーザ管理部 18 が集めたコンテンツの利用の実績を示す情報である課金情報、必要に応じてそのコンテンツに対応する価格情報 (サービスプロバイダ 3 から送られてくるものと、ユーザが課金情報に付加して送ってくるものの、どちらか一方又は両方)、および必要に応じてそのコンテンツに対応する取扱方針 (コンテンツプロバイ

ダ2から送られてくるものと、ユーザが課金情報に付加して送ってくるものの、どちらか一方又は両方)を保持・管理し、サービスプロバイダ管理部11又はコンテンツプロバイダ管理部12等が課金情報や利用履歴等を利用する際にデータを出力する。なお、価格情報及び取扱方針は、課金情報に必要なデータが書き込まれている場合サービスプロバイダ3やコンテンツプロバイダ2から送られてこない場合がある。利益分配部16は、経歴データ管理部15から供給された、課金情報、必要に応じて価格情報、および取扱方針に基づき、電子配信サービスセンタ1、コンテンツプロバイダ2、およびサービスプロバイダ3の利益を算出する。これらの情報は、出納部20へ供給され、出納部20を介して利益分配を行う場合もあるが、利益分配を行わず、これらの情報のみをサービスプロバイダ管理部11、コンテンツプロバイダ管理部12、著作権管理部13に送信し、売上そのものはサービスプロバイダに入金させ、サービスプロバイダ3が各受益者に利益を分配する場合がある。相互認証部17は、コンテンツプロバイダ2、サービスプロバイダ3、およびユーザホームネットワーク5の所定の機器と後述する相互認証を実行する。

ユーザ管理部18は、ユーザ登録データベースを有し、ユーザホームネットワーク5の機器から登録の要求があったとき、ユーザ登録データベースを検索し、その記録内容に応じて、その機器を登録したり、または登録を拒否する等の登録情報を作成する。ユーザホームネットワーク5が電子配信サービスセンタ1と接続が可能な機能を有する複数の機器から構成されているとき、ユーザ管理部18は、登録情報に決済をする機器を規定し、決済IDを登録し、更に、コンテンツの購入処理動作を規定したり、ユーザホームネットワークを構成する機器の範囲を規定したり、取引停止等の情報を規定し、ユーザホームネットワーク5の所定の機器(決済可能機器)に送信する。

図7に示すユーザ登録データベースの例は、ユーザホームネットワーク5内で構築されたネットワークグループ毎の登録状況を示したもので、各グループには、グループのIDを示すグループID、ホームネットワーク5を構成する機器に

固有のID、そのIDに対応して（すなわち、そのIDを有する機器毎に）、電子配信サービスセンタ1と接続が可能か否か、決済処理可能か否か、コンテンツの購入ができるか否か、決済処理を行うのはどの機器か、コンテンツの購入を依頼する機器はどれか、登録可能か否か、等の情報を記録する。

ユーザ登録データベースに記録されたグループIDはユーザホームネットワーク毎に割り振られ、このグループ単位で決済、情報更新が行われる。従って、原則的にはグループ内の代表機器が電子配信サービスセンタ1と通信、決済処理、情報更新を一括して行い、グループ内の他の機器は電子配信サービスセンタ1とのやりとりを直接は行わない。ユーザ登録データベースに記録されたIDは、機器毎に個別に割り振られたIDで、機器を識別するのに使用される。

ユーザ登録データベースに記録された電子配信サービスセンタ1と接続が可能か否かの情報は、その機器が、電子配信サービスセンタ1と物理的に接続が可能であるか否かを示し、接続できると記録された機器でも、決済処理可能であるとされた機器以外は、原則的に電子配信サービスセンタ1に接続されることがない（ただし、グループ内の代表機器が何らかの原因で決済処理動作しなくなった場合、代理で一時的に電子配信サービスセンタ1に接続されることはある）。また、接続ができないと記録された機器は、ユーザホームネットワーク5の決済処理可能な機器を介して、電子配信サービスセンタ1に、課金情報等を出力する。

ユーザ登録データベースに記録された決済処理が可能か否かの情報は、その機器が、決済可能か否かを示す。ユーザホームネットワーク5が、コンテンツの利用権の購入などが可能な複数の機器で構成されているとき、その中の決済処理が可能である1台の機器は、電子配信サービスセンタ1に、ユーザホームネットワーク5の電子配信サービスセンタ1に登録されている全ての機器の、課金情報、必要に応じて価格情報、および取扱方針を送信し、決済処理の完了に応じて電子配信サービスセンタ1から配送鍵K<sub>d</sub>、登録情報を受信する。こうすることで、機器毎に処理を行うのに比べ、電子配信サービスセンタ1の処理が軽減される。

ユーザ登録データベースに記録された購入処理が可能か否かの情報は、その機

器が、コンテンツの利用権の購入ができるか否かを表す。購入不可の機器においては、他の購入可の機器から利用権の代理購入（別の機器で権利を購入し、その権利を全て譲り受けるものを言う。供給側には全く権利は残らない）、再配布（既に購入したコンテンツの利用権を、同一利用権内容または異なる利用権内容でもう一度購入し、別機器に供給する方式を言う。このとき、供給側には全く権利は残らない。再配布は、割引を行うことを主たる目的とする。割引の特典を受けられるのは、同一決済IDを使用しているグループであることが条件である。なぜなら、同一決済IDに属するグループ内の処理においては、電子配信サービスセンタ1の処理負担が軽減され、従って、その代償として割引が受けられるからである）または管理移動（コンテンツ再生権、特に無期限再生権の移動ができるが、再生権送信器においては再生権受信器がどの機器であるか管理され、再生権の返還がない場合、再度管理移動ができず、再生権受信器においては、再生権送信器がどの機器であるかが管理され、再度管理移動が全くできず、唯一、再生権を与えてくれた再生権送信器に再生権を返還することのみできる）を行ってもらってコンテンツ利用権を取得する。

ここで、コンテンツの利用方法／利用権及び購入方法について簡単に説明する。コンテンツの利用方法としては、コンテンツの利用権を自己で管理保持しているものが利用する場合と、他機器の保持する利用権を行使して自己の機器において利用する、2つのものがある。コンテンツの利用権としては、無制限再生権（コンテンツの再生期間及び回数に制限がないもの、なお、音楽コンテンツの場合は再生であるが、ゲームプログラム等では実行になる）、時間制限付き再生権（コンテンツの再生できる期間が限られているもの）、回数制限付き再生権（コンテンツの再生できる回数が限られているもの）、無制限複製権（コンテンツの複製期間及び回数に制限がないもの）、回数制限付き複製権（コンテンツの複製に回数制限があるもの）（複製権には、コピー管理情報なし複製権、コピー管理情報付き複製権（SCMS）等、その他専用メディア向け複製権等がある）（また時間制限付き複製権もある場合がある）、管理移動権がある。そして、利用権の購入方法としては



、これらの利用権を直接購入する通常の購入に加え、既に購入した利用権の内容を別の内容に変更する利用権内容変更、他の機器で既に購入した権利に基づき利用権を別途購入する再配布、他の機器で利用権の購入を代理で行ってもらう代理購入、複数のコンテンツ利用権を一括して購入管理するアルバム購入等がある。

ユーザ登録データベースに記録された代理決済者に記された情報は、コンテンツの利用権を購入した際に生成した課金情報を、代理で電子配信サービスセンタ 1 に送信してもらう機器の ID を示す。

ユーザ登録データベースに記録された代理購入者に記された情報は、コンテンツの利用権の購入ができない機器に対し、代理で利用権の購入を行ってくれる機器の ID を示す。ただし、購入処理可能なグループ内機器全てが代理購入者ということにしてした場合には、特に記録しておく必要はない。

ユーザ登録データベースに記録された登録が可能か否かの情報は、決済機関(例えば、銀行)、またはクレジットカード会社などから供給される料金の未払い、不正処理等の情報を基に、更新される。登録が不可と記録された ID を有する機器の登録の要求に対して、ユーザ管理部 18 は、その登録を拒否し、登録を拒否された機器は、以降、このシステムのコンテンツの購入ができないだけでなく、ユーザホームネットワーク 5 内の他機器とのデータ送受信もできなくなる。また場合によっては購入済のコンテンツの利用も制限される場合がある(ただし、電子配信サービスセンタ 1 等に機器を持ち込み、検査等を済ませた後再登録されることはある)。また、「登録可」、「登録不可」だけでなく、「決済未処理」、「一時停止」等の状態もあり得る。

また、ユーザ管理部 18 は、ユーザホームネットワーク 5 の機器から課金情報、登録情報、必要に応じて価格情報や取扱方針が供給され、課金情報、価格情報、および取扱方針を経歴データ管理部 15 に出力し、ユーザホームネットワーク 5 の機器に、配送鍵 K<sub>j</sub>、登録情報を供給する。供給されるタイミングについては後述する。

ここで、図 8 を用いて登録情報を説明する。図 8 の登録情報はユーザ登録デー

データベースの情報に加え、決済IDおよび署名が付加されており、同一決済グループの情報のみが含まれている。決済IDとは、決済を行う際に課金請求部19および出納部20が使用するユーザの、ユーザ情報データベース（例えば銀行口座番号やクレジットカード番号）内のIDを示している。署名の生成については、後述する。

再び図2にもどり、課金請求部19は、経歴データ管理部15から供給された、課金情報、必要に応じて価格情報、および取扱方針に基づき、ユーザへの課金を算出し、その結果を、出納部20に供給する。また、必要に応じてユーザ管理部18を介してユーザに決済情報を提供する。出納部20は、ユーザ、コンテンツプロバイダ2、およびサービスプロバイダ3への出金、徴収すべき利用料金の金額を基に、図示せぬ外部の銀行等と通信し、決済処理を実行する。なお、出納部20は、サービスプロバイダ3へ売上のすべてを送金させ、利益分配部16を介して送信された分配金情報をもとに、サービスプロバイダ3が利益分配をする場合がある。監査部21は、ユーザホームネットワーク5の機器から供給された課金情報、価格情報、および取扱方針を、コンテンツプロバイダ2から供給された取扱方針と、サービスプロバイダ3から供給された価格情報とからその正当性を監査する。

また、監査部21の処理としては、ユーザホームネットワーク5から入金された金額と、利益分配した合計金額又はサービスプロバイダ3へ送った金額との整合性を監査する処理や、ユーザホームネットワーク5の機器から供給された課金情報内のデータに例えば存在し得ないコンテンツプロバイダID、サービスプロバイダIDや考えられない取り分、価格等が含まれているか否かを監査する処理がある。

認証局22は、鍵サーバ14から供給された公開鍵の証明書を作成し、コンテンツプロバイダ2、サービスプロバイダ3へ供給し、ユーザ機器製造時にホームサーバ51の大容量記憶部68（後述する）や、据置機器52の小容量記憶部75（後述する）に保存される公開鍵証明書も生成する。コンテンツプロバイダ2

がコンテンツのオーサリングを行わない場合、これを代替える方法として、コンテンツを保持するコンテンツサーバ23、コンテンツオーサリング24がある。

図9は、コンテンツプロバイダ2の機能の構成を示すブロック図である。コンテンツサーバ31は、ユーザに供給するコンテンツを記憶し、電子透かし（ウォーターマーク）付加部32に供給する。電子透かし付加部32は、コンテンツサーバ31から供給されたコンテンツに自分の所有物であることを示すコンテンツプロバイダIDを電子透かしの形で挿入し、圧縮部33に供給する。圧縮部33は、電子透かし付加部32から供給されたコンテンツを、ATRAC（Adaptive Transform Acoustic Coding）（商標）等の方式で圧縮し、コンテンツ暗号手段であるコンテンツ暗号部34に供給する。因に、圧縮方式としてはATRACに代えてMP3やAAC等の方式を用いることができる。コンテンツ暗号部34は、圧縮部33で圧縮されたコンテンツを、コンテンツ鍵生成部35から供給された鍵（以下、この鍵をコンテンツ鍵 $K_c$ と称する）を用いて、DES（Data Encryption Standard）などの共通鍵暗号方式で暗号化し、その結果を送信手段である署名生成部38に出力する。

コンテンツ鍵生成部35は、コンテンツ鍵 $K_c$ となる所定のビット数の乱数を生成し、この中で弱鍵（例えば、 $K_c=1E1E1E1E0E0E0E0E$ や $1EE01EE00EF00EF0$ など）と呼ばれる暗号化に不適なビット列を除いたものをコンテンツ暗号部34、コンテンツ鍵暗号部36に供給する。そのような不適なビット列がない暗号アルゴリズムを使用するときは、不適なビット列を除く処理は不要である。コンテンツ鍵暗号部36は、コンテンツ鍵 $K_c$ を電子配信サービスセンタ1から供給された個別鍵 $K_i$ を使用して、DESなどの共通鍵暗号方式で暗号化し、その結果を署名生成部38に出力する。因に、暗号化方式としては、DESに限らず、例えばRSA（Rivest, Shamir, Adleman）等の公開鍵暗号方式を用いるようにしても良い。

DESは、56ビットの共通鍵を用い、平文の64ビットを1ブロックとして処理する暗号方式である。DESの処理は、平文を攪拌し、暗号文に変換する部分（データ攪拌部）と、データ攪拌部で使用する鍵（拡大鍵）を共通鍵から生成する部分（鍵処理部）からなる。DESの全てのアルゴリズムは公開されているので、ここでは、データ攪拌部の基本的な処理を簡単に説明する。

まず、平文64ビットは、上位32ビットのH0、および下位32ビットのL0に分割される。鍵処理部から供給された48ビットの拡大鍵K1、および下位32ビットのL0を入力として、下位32ビットのL0を攪拌したF関数の出力が算出される。F関数は、数値を所定の規則で置き換える「換字」およびビット位置を所定の規則で入れ替える「転置」の2種類の基本変換から構成される。次に、上位32ビットのH0と、F関数の出力が排他的論理和され、その結果はL1とされる。L0は、H1とされる。

上位32ビットのH0および下位32ビットのL0を基に、以上の処理を16回繰り返し、得られた上位32ビットのH16および下位32ビットのL16が暗号文として出力される。復号は、暗号化に使用した共通鍵を用いて、上記の手順を逆にたどることで実現される。

なお、本実施の形態では共通鍵暗号としてDESを示したが、NTT（商標）が提案するFEAL（Fast Encryption Algorithm）、IDEA（International Data Encryption Algorithm）、E2や、米国次期暗号標準であるAES（Advanced Encryption Standard）など、いずれでもよい。

取扱方針生成部37は、コンテンツの取扱方針を生成し、暗号化されるコンテンツに対応して、取扱方針を署名生成部38に出力する。なお、取扱方針生成部37は、生成した取扱方針を図示せぬ通信手段を介して電子配信サービスセンタ1に供給する場合があり、そのデータは保持・管理されている。署名生成部38は、暗号化されたコンテンツ、暗号化されたコンテンツ鍵K<sub>o</sub>、暗号化された個

別鍵 $K_i$ 、取扱方針に電子署名を付加し、コンテンツプロバイダ2の証明書 $C_c$ と共にサービスプロバイダ3に送信する（以降、暗号化されたコンテンツ、暗号化されたコンテンツ鍵 $K_c$ 、暗号化された個別鍵 $K_i$ 、取扱方針のそれぞれにコンテンツプロバイダ3の秘密鍵を使用して電子署名を付加したものを、コンテンツプロバイダセキュアコンテナと称する）。なお、個々のデータに署名を別々に付加するのではなく、データ全体に対して1つの署名を付けるようにしてもよい。

相互認証部39は、電子配信サービスセンタ1と相互認証し、また、必要に応じてサービスプロバイダ3へのコンテンツプロバイダセキュアコンテナの送信に先立ち、サービスプロバイダ3と相互認証する。メモリ40Aは、コンテンツプロバイダ2が秘密裏に保持しなくてはならない個別鍵 $K_i$ を保持するため、第三者に容易にデータを読み出されない耐タンパメモリが望ましいが、特にハードウェア的制限は必要ない（例えば、入室管理された部屋の中にあるハードディスクや、パスワード管理されたパソコンのハードディスク等でよい）。また、メモリ40Bは、配送鍵 $K_d$ で暗号化された個別鍵 $K_i$ 、コンテンツプロバイダ2の公開鍵証明書が保存されるだけであるため、通常の記憶装置等何でもよい（公開情報であるため、秘密にする必要がない）。なお、メモリ40A、40Bを一つにしてもかまわない。

署名は、データまたは後述する証明書に付け、改竄のチェックおよび作成者認証をするためのデータであり、送信したいデータを基にハッシュ関数でハッシュ値をとり、これを公開鍵暗号の秘密鍵を使用して作成される。

ハッシュ関数および署名について説明する。ハッシュ関数は、送信したい所定のデータを入力とし、所定のビット長のデータに圧縮し、ハッシュ値として出力する関数である。ハッシュ関数は、ハッシュ値（出力）から入力を予測することが難しく、ハッシュ関数に入力されたデータの1ビットが変化したとき、ハッシュ値の多くのビットが変化し、また、同一のハッシュ値を持つ入力データを探し出すことが困難である特徴を有する。ハッシュ関数としては、MD (Message Digest) 4、MD5、SHA (Secure Hash

Algorithm) - 1などが用いられる。

データと署名を送信する送信装置（コンテンツプロバイダ2）の署名生成部38は、例えば、公開鍵暗号方式である楕円曲線暗号を用いて署名を生成する。この処理を、図10を用いて説明する（ECDSA（Elliptic Curve Digital Signature Algorithm）、IEEE P1363/D3）。ステップS1で、Mをメッセージ、pを標数、a、bを楕円曲線の係数（楕円曲線： $y^2 = x^3 + ax + b$ ）、Gを楕円曲線上のベースポイント、rをGの位数、 $K_s$ を秘密鍵（ $0 < K_s < r$ ）とする。ステップS2で乱数uを $0 < u < r$ になるように乱数発生ユニットで生成する。ステップS3でベースポイントをu倍した座標を計算する。なお、楕円曲線上の加算、2倍算は次のように定義されている。

$P = (X_0, Y_0)$ 、 $Q = (X_1, Y_1)$ 、 $R = (X_2, Y_2) = P + Q$ とし、 $P \neq Q$ の時、

$$X_2 = \lambda^2 - X_0 - X_1$$

$$Y_2 = \lambda (X_0 - X_2) - Y_0$$

$$\lambda = (Y_1 - Y_0) / (X_1 - X_0)$$

$P = Q$ の時、

$$X_2 = \lambda^2 - 2X_0$$

$$Y_2 = \lambda (X_0 - X_2) - Y_0$$

$$\lambda = (3X_0^2 + a) / 2Y_0$$

となり、これらを用いて点Gのu倍を計算する（速度は遅いが、最もわかりやすい演算方法として次のように行う。G、2G、4G・・・を計算し、uを2進数展開して1が立っているところに対応する（ $2^i$ ）×Gを加算する（iはuのLSBから数えた時のビット位置））。ステップS4で $c = X_v \bmod r$ を計算し、ステップS5でこの値が0になるかどうか判定し、0でなければステップS6へと進み、メッセージMのハッシュ値を計算し、 $f = \text{SHA-1}(M)$ とする。次に、ステップS7において、 $d = [(f + cK_s) / u] \bmod r$ を計算

し、ステップS 8でdが0であるかどうか判定する。dが0出なければ、cおよびdを署名データとする。仮に、rを160ビット長の長さであると仮定すると、署名データは320ビット長となる。

ステップS 5において、cが0であった場合、ステップS 2に戻って新たな乱数を生成し直す。同様に、ステップS 8でdが0であった場合も、ステップS 2に戻って乱数を生成し直す。

署名とデータを受信した受信装置（ユーザホームネットワーク5）は、例えば、公開鍵暗号方式である楕円曲線暗号を用いて署名を検証する。この処理を、図11を用いて説明する。（受信装置は）ステップS 10で、Mをメッセージ、pを標数、a、bを楕円曲線の係数（楕円曲線： $y^2 = x^3 + ax + b$ ）、Gを楕円曲線上のベースポイント、rをGの位数、Gおよび $K_s$ 、Gを公開鍵（ $0 < K_s < r$ ）とする。ステップS 11で署名データcおよびdが $0 < c$ 、 $d < r$ を満たすか検査する。これを満たしていた場合、ステップS 12で、メッセージMのハッシュ値を計算し、 $f = \text{SHA-1}(M)$ とする。次に、ステップS 13で $h = 1 / d \bmod r$ を計算し、ステップS 14で $h_1 = fh$ 、 $h_2 = ch \bmod r$ を計算する。ステップS 15において、既に計算した $h_1$ および $h_2$ を用い、 $P = (X_p, Y_p) = h_1 G + h_2 K_s$ を計算する。署名検証者は、公開鍵Gおよび $K_s$ を知っているので、ステップS 3と同様にこの計算ができる。そして、ステップS 16でPが無限遠点かどうか判定し、無限遠点でなければステップS 17に進む（実際には、無限遠点の判定はステップS 15でできてしまう。つまり、 $P = (X, Y)$ 、 $Q = (X, -Y)$ の加算を行うと、前述のλが計算できず、Rが無限遠点であることが判明している。ステップS 17で $X_p \bmod r$ を計算し、署名データcと比較する。この値が一致していた場合、ステップS 18に進み、署名が正しいと判定する。

署名が正しいと判定された場合、受信データは改竄されておらず、公開鍵に対応した秘密鍵を保持する送信装置から送信されたデータであることがわかる。

ステップS 11において、署名データcおよびdが $0 < c$ 、 $d < r$ を満たさな

かった場合、ステップS 1 9に進む。また、ステップS 1 6において、Pが無限遠点であった場合もステップS 1 9に進む。さらにまた、ステップS 1 7において、 $X_p \bmod r$ の値が、署名データcと一致していなかった場合にもステップS 1 9に進む。ステップS 1 9において、署名が正しくないと判定する。

署名が正しくないと判定された場合、受信データは改竄されているか、公開鍵に対応した秘密鍵を保持する送信装置から送信されたデータではないことがわかる。

なお、本実施の形態では、ハッシュ関数としてSHA-1を使用したか、MD 4、MD 5などいずれの関数を使用してもよい。また、署名の生成および検証はRSA暗号を用いて行ってもよい(ANSI X9.31-1)。

次に公開鍵暗号方式の暗号化・復号化について説明する。暗号化および復号化で同一の鍵(共通鍵)を使用する共通鍵暗号方式に対して、公開鍵暗号方式は、暗号化に使用する鍵と復号化に使用する鍵が異なる。公開鍵暗号方式を用いる場合、鍵の一方を公開しても他方を秘密に保つことができ、公開してもよい鍵は、公開鍵と称され、他方の秘密に保つ鍵は、秘密鍵と称される。

公開鍵暗号方式の中で代表的な楕円曲線暗号化方法を説明する。図1 2において、ステップS 2 0で、 $M_x$ 、 $M_y$ をメッセージ、 $p$ を標数、 $a$ 、 $b$ を楕円曲線の係数(楕円曲線： $y^2 = x^3 + ax + b$ )、 $G$ を楕円曲線上のベースポイント、 $r$ を $G$ の位数、 $G$ および $K_r G$ を公開鍵( $0 < K_r < r$ )とする。ステップS 2 1で乱数 $u$ を $0 < u < r$ になるように生成する。ステップS 2 2で公開鍵 $K_r G$ を $u$ 倍した座標 $V$ を計算する。なお、楕円曲線上のスカラー倍は署名生成のところで説明した方法と同一のため、ここでは説明を省略する。ステップS 2 3で、 $V$ の $X$ 座標を $M_x$ 倍して $p$ で剰余を求め $X_0$ とする。ステップS 2 4で $V$ の $Y$ 座標を $M_y$ 倍して $p$ で剰余を求め $Y_0$ とする。なお、メッセージの長さが $p$ のビット数より少ない場合、 $M_y$ は乱数を使い、復号部では $M_y$ を破棄するようにする。ステップS 2 5において、 $uG$ を計算し、ステップS 2 6で暗号文 $uG$ 、 $(X_0$ 、 $Y_0)$ を得る。



ここで公開鍵暗号方式の復号化について、図13を用いて説明する。ステップS30において、 $uG$ 、 $(X_0, Y_0)$ を暗号文データ、 $p$ を標数、 $a$ 、 $b$ を楕円曲線の係数（楕円曲線： $y^2 = x^3 + ax + b$ ）、 $G$ を楕円曲線上のベースポイント、 $r$ を $G$ の位数、 $K_s$ を秘密鍵（ $0 < K_s < r$ ）とする。ステップS31において、暗号データ $uG$ を秘密鍵 $K_s$ 倍する。ステップS32では、暗号データの内、 $(X_0, Y_0)$ の $X$ 座標を取り出し、 $X_1 = X_0 / X_s \bmod p$ を計算する。ステップS33においては、 $Y_1 = Y_0 / Y_s \bmod p$ を計算する。そして、ステップS34で $X_1$ を $M_x$ とし、 $Y_1$ を $M_y$ としてメッセージを取り出す。この時、 $M_y$ をメッセージにしていなかった場合、 $Y_1$ は破棄する。

このように公開鍵暗号方式では、秘密鍵を $K_s$ 、公開鍵を $G$ 、 $K_s G$ とすることで、暗号化に使用する鍵と復号化に使用する鍵を、異なる鍵とすることができる。

また、公開鍵暗号方式の他の例としてはRSA暗号（Rivest, Shamir, Adleman）が知られている。

図14は、サービスプロバイダ3の機能の構成を示すブロック図である。コンテンツサーバ41は、コンテンツプロバイダ2から供給された、コンテンツプロバイダ2の公開鍵証明書および暗号化されているコンテンツを記憶している。コンテンツプロバイダ2の公開鍵証明書は、証明書検査部42で、証明書内の署名が認証局22の公開鍵で検証され、検証に成功した場合、コンテンツプロバイダ2の公開鍵を署名検証部43に供給する。署名検証部43においては、コンテンツサーバ41に記憶されている取扱方針に対するコンテンツプロバイダ2の署名を、先ほど検証したコンテンツプロバイダ2の公開鍵を用いて検証し、検証に成功した場合、取扱方針を値付け部44に供給する。値付け部44においては、取扱方針から価格情報を作成し、署名生成部45に供給する。署名生成部45においては、図示せぬ耐タンパメモリ（コンテンツプロバイダ2内の40Aと同様）に保持されたサービスプロバイダ3の秘密鍵を用い、価格情報に対する署名を生成する（以降、コンテンツプロバイダセキュアコンテナおよび価格情報にサービ

スプロバイダ3の秘密鍵を用いて電子署名を付加したものを、サービスプロバイダセキュアコンテナと称する)。なお、価格情報に署名を付加するのではなく、コンテンツプロバイダセキュアコンテナと価格情報全体に対して1つの署名を生成するようにしてもよい。そして、サービスプロバイダセキュアコンテナ、コンテンツプロバイダ2の公開鍵証明書、サービスプロバイダ3の公開鍵証明書を、ネットワーク4(図1)を介してユーザホームネットワーク5へ供給する。相互認証部46は、電子配信サービスセンタ1と相互認証し、また、必要に応じてコンテンツプロバイダ、およびインターネット、ケーブル通信等を介し、可能であればユーザホームネットワーク5と相互認証する。

図15は、ユーザホームネットワーク5の構成を示すブロック図である。ホームサーバ51は、ネットワーク4を介して、サービスプロバイダ3からコンテンツを含んだセキュアコンテナを受信し、コンテンツの利用権を購入し、その権利を行使してコンテンツの復号、伸張、再生、複製を行う。

通信部61は、ネットワーク4を介してサービスプロバイダ3、または電子配信サービスセンタ1と通信し、所定の情報を受信し、または送信する。上位コントローラ62は、入力手段63からの信号を受信し、所定のメッセージ等を表示手段64に表示し、暗号処理部65を利用してコンテンツの利用権購入処理等を行い、伸張部66に大容量記憶部68から読み出した暗号化されたコンテンツを供給し、大容量記憶部68に暗号化されたコンテンツ等を記憶する。入力手段63は、リモートコントローラからの信号や入力ボタンからの入力データを上位コントローラ62に送信する。表示手段64は、液晶表示器のような表示デバイスで構成され、ユーザに指示を出したり、情報を表示したりする。入力手段63および表示手段64は、必要に応じてタッチパネル式液晶表示器などになり、一つにまとめられる場合がある。暗号処理部65は、サービスプロバイダ3、または電子配信サービスセンタ1若しくはその他の機器の暗号処理部と相互認証し、コンテンツ利用権を購入すると共に、所定のデータの暗号化/復号化を行い、コンテンツ鍵 $K_c$ 、および使用許諾条件情報を保持する外部メモリを管理し、さらに配

送鍵 $K_d$ 、課金情報等を記憶する。伸張部66は、暗号処理部65と相互認証してコンテンツ鍵 $K_c$ を受信し、このコンテンツ鍵 $K_c$ を用いて上位コントローラ62から供給された暗号化されたコンテンツを復号化し、ATRA C等の所定の方式で伸張し、さらに所定の電子透かしをコンテンツに挿入する。外部メモリ67は、フラッシュメモリ等の不揮発メモリやバックアップ電源付き揮発性メモリで構成され、保存鍵 $K_{sav}$ で暗号化されたコンテンツ鍵 $K_c$ および使用許諾条件情報を保存する。大容量記憶部68はHDDや光ディスク等の記憶デバイスで、コンテンツプロバイダセキュアコンテナおよびサービスプロバイダセキュアコンテナ（暗号化されたコンテンツ、個別鍵 $K_i$ で暗号化されたコンテンツ鍵 $K_c$ 、配送鍵 $K_d$ で暗号化された個別鍵 $K_i$ 、取扱方針、価格情報及びそれらの署名）、公開鍵証明書、登録情報等が保存されている。

電子配信サービスセンタ1と相互認証し、コンテンツ利用権を購入すると共に課金情報を生成し、所定のデータの復号化／暗号化を行い、コンテンツ鍵 $K_c$ および使用許諾条件情報を保持する外部メモリを管理し、さらに配送鍵 $K_d$ 、課金情報等を記憶する暗号処理部65は、制御部91、記憶モジュール92、登録情報検査モジュール93、購入処理モジュール94、相互認証モジュール95、暗号／復号化モジュール96、および外部メモリ制御部97から構成される。この暗号処理部65は、シングルチップの暗号処理専用ICで構成され、多層構造を有し、その内部のメモリセルはアルミニウム層等のダミー層に挟まれ、また、動作する電圧または周波数の幅が狭い等、外部から不正にデータが読み出し難い特性（耐タンパ性）を有する。

制御部91は、上位コントローラ62からのコマンドに応じて各モジュールを制御すると共に、各モジュールからの結果を上位コントローラ62に返送する。記憶モジュール92は、購入処理モジュール94から供給された課金情報、および配送鍵 $K_d$ 等のデータを記憶し、他の機能ブロックが所定の処理を実行するとき、配送鍵 $K_d$ 等のデータを供給する。登録情報検査モジュール93は、上位コントローラ62から供給された登録情報を検査し、ユーザホームネットワーク5

内の他の機器と相互認証するか否か、課金情報の授受をすべきか否か、コンテンツの再配布等をすべきか否かの判断を行う。購入処理モジュール 9 4 は、サービスプロバイダ 3 から受信したセキュアコンテナに含まれる取扱方針および価格情報（並びに、場合によっては、既に保持している使用許諾条件情報）から、新たに使用許諾条件情報を生成して外部メモリ制御部 9 7 又は制御部 9 1 に出力し、課金情報を生成して記憶モジュール 9 2 に出力する。相互認証モジュール 9 5 は、電子配信サービスセンタ 1、ホームネットワーク 5 内の他の機器の暗号処理部および伸張部 6 6 との相互認証を実行し、必要に応じて、一時鍵  $K_{temp}$ （セッション鍵）を生成し、暗号／復号化モジュール 9 6 に供給する。

復号／暗号化モジュール 9 6 は、復号化ユニット 1 1 1、暗号化ユニット 1 1 2、乱数発生ユニット 1 1 3、署名生成ユニット 1 1 4、および署名検証ユニット 1 1 5 から構成される。復号化ユニット 1 1 1 は、配送鍵  $K_d$  で暗号化された個別鍵  $K_i$  を復号化したり、個別鍵  $K_i$  で暗号化されたコンテンツ鍵  $K_c$  を復号化したり、一時鍵  $K_{temp}$  で暗号化された各種データを復号化したりする。暗号化ユニット 1 1 2 は、復号化されたコンテンツ鍵  $K_c$  を、記憶モジュール 9 2 に保持されている保存鍵  $K_{save}$  で暗号化し、制御部 9 1 を介して外部メモリ制御部 9 7 に出力したり、一時鍵  $K_{temp}$  で各種データを暗号化したりする。乱数発生ユニット 1 1 3 は、所定の桁数の乱数を発生し、相互認証モジュール 9 5 や署名生成ユニット 1 1 4 に供給する。署名生成ユニット 1 1 4 は、制御部 9 1 から供給されたメッセージのハッシュ値を計算し、乱数発生ユニット 1 1 3 から供給された乱数を用いて署名データを生成して制御部 9 1 に出力する。署名検証ユニット 1 1 5 は、制御部から供給されたメッセージおよび署名データから署名が正しいかどうか判定し、その結果を制御部 9 1 に出力する。なお、署名の生成／検証方法については図 1 0、図 1 1 について上述した場合と同様である。

外部メモリ制御部 9 7 は、外部メモリ 6 7 を制御してデータの読み書きを行い、外部メモリ内のデータが改竄されていないかどうかデータ検証を行う。図 1 6 は、外部メモリ制御部 9 7 の動作を説明するブロック図である。図 1 6 において

、記憶モジュール 92 には、N 個の改竄防止用ハッシュ値 ( Integrity Check Value ) が保存されている。外部メモリ 67 は、N ブロックのデータ領域に分割されており、それぞれのデータ領域には M 組のコンテンツ鍵  $K_{\circ}$ 。および使用許諾条件情報が書き込めるようになっている。また、外部メモリ 67 には、自由に使用できるその他の領域も用意されている。改竄防止用ハッシュ値 ICV は、それに対応する外部メモリ 67 内の全データに対するハッシュ値になっている。外部メモリの読み出し手順および書き込み手順については、フローチャートを用いて後述する。

コンテンツを復号化し、伸張し、所定の電子透かしを付加する伸張部 66 ( 図 15 ) は、相互認証モジュール 101、鍵復号モジュール 102、復号モジュール 103、伸張モジュール 104、電子透かし付加モジュール 105、および記憶モジュール 106 から構成される。相互認証モジュール 101 は、暗号処理部 65 と相互認証し、一時鍵  $K_{temp}$  を鍵復号モジュール 102 に出力する。鍵復号モジュール 102 は、外部メモリ 67 から読み出され一時鍵  $K_{temp}$  で暗号化されているコンテンツ鍵  $K_{\circ}$ 。を一時鍵  $K_{temp}$  で復号化し、復号モジュール 103 に出力する。復号モジュール 103 は、大容量記憶部 68 に記録されたコンテンツをコンテンツ鍵  $K_{\circ}$ 。で復号化し、伸張モジュール 104 に出力する。伸張モジュール 104 は、復号化されたコンテンツを、更に ATRAC 等の方式で伸張し、電子透かし付加モジュール 105 に出力する。電子透かし付加モジュール 105 は、購入処理を行った暗号処理部の個別 ID を電子透かし技術を用いてコンテンツに挿入し、他の機器や図示せぬスピーカに出力し、音楽を再生する。

記憶モジュール 106 には、暗号処理部 65 との相互認証に必要な鍵データが保存されている。なお、伸張部 66 は、耐タンパ性を備えていることが望ましい。

外部メモリ 67 は、購入処理モジュール 94 で権利購入した際に生成した使用許諾条件情報や保存鍵  $K_{save}$  で暗号化されたコンテンツ鍵  $K_{\circ}$ 。を記憶している。大容量記憶部 68 は、サービスプロバイダ 3 から供給されたセキュアコンテナや公

開鍵証明書、登録情報等を記録する。

装着された光ディスク、半導体メモリ等の記録メディア80にサービスプロバイダ3から供給されたコンテンツを記録し、再生する据置機器52は、通信部71、上位コントローラ72、暗号処理部73、伸張部74、小容量記憶部75、記録再生部76、入力手段77、表示手段78、外部メモリ79、および記録メディア80から構成される。通信部71は通信部61と同じ機能を有し、その説明は省略する。上位コントローラ72は上位コントローラ62と同じ機能を有し、その説明は省略する。暗号処理部73は暗号処理部65と同じ機能を有し、その説明は省略する。伸張部74は伸張部66と同じ機能を有し、その説明は省略する。小容量記憶部75は大容量記憶部68と同じ機能を有しているものの、コンテンツそのものは保存されず、公開鍵証明書や登録情報等が記憶されるだけである。記録再生部76は、光ディスク、半導体メモリ等の記録メディア80が装着され、その記録メディア80にコンテンツを記録し、読み出したコンテンツを伸張部に出力する。入力手段77は入力手段63と同じ機能を有し、その説明は省略する。表示手段78は表示手段64と同じ機能を有し、その説明は省略する。外部メモリ79は外部メモリ67と同じ機能を有し、その説明は省略する。記録メディア80は、例えばMD (Mini Disk : 商標) や、電子配信専用記憶メディア (半導体メモリを用いたMemory Stick : 商標) であつたりする。

ユーザが携帯し、音楽を再生して楽しむための機器である携帯機器53は、通信部81、上位コントローラ82、暗号処理部83、伸張部84、および外部メモリ85から構成される。通信部81は通信部61と同じ機能を有し、その説明は省略する。上位コントローラ82は上位コントローラ62と同じ機能を有し、その説明は省略する。暗号処理部83は暗号処理部65と同じ機能を有し、その説明は省略する。伸張部84は伸張部66と同じ機能を有し、その説明は省略する。外部メモリ85は外部メモリ67と同じ機能を有し、その説明は省略する。ただし、これらのメモリは半導体メモリだけとは限らず、HDD、書き換え可能

な光ディスク等いずれでもよい。

図 1 7 は、電子配信専用の記録メディアの構成図を示したものである。電子配信されたコンテンツを保存する記録メディア 1 2 0 は、通信部 1 2 1、暗号処理部 1 2 2、および外部メモリ 1 2 3 から構成される。通信部 1 2 1 は、据置機器 5 2（図 1 5）の記録再生部 7 6 とデータの送受信を行う。据置機器 5 2 と相互認証し、コンテンツ利用権を譲り受け、所定のデータの復号化／暗号化を行い、コンテンツ鍵  $K_{co}$  および使用許諾条件情報等を保持する外部メモリを管理し、さらに保存鍵  $K_{save}$  等を記憶する暗号処理部 1 2 2 は、その構成は暗号処理部 6 5 と同じ機能を有し、その説明は省略する。外部メモリ 1 2 3 は、保存鍵  $K_{save}$  で暗号化されたコンテンツ鍵  $K_{co}$ 、コンテンツ鍵  $K_{co}$  で暗号化されたコンテンツ、コンテンツの使用条件を定めた使用許諾条件情報、必要に応じて取扱方針、および価格情報を記憶している。

電子配信専用記録メディア 1 2 0 は、据置機器 5 2 の時に説明した記録メディアとは使い方が異なっている。通常の記録メディア 8 0 は、ホームサーバ 5 1 の大容量記憶部 6 8 の代用品であるのに対し、電子配信専用メディア 1 2 0 は、伸張部を持たない携帯機器に異ならない。従って、コンテンツの再生を行う際には、伸張部 7 4 をもつ据置機器 5 2 のような機器が必要であるが、コンテンツを譲り受けたり、コンテンツを管理したりする機能に関してはホームサーバ 5 1 や携帯機器 5 3 と同様な処理ができる。これらの違いにより、通常の記録メディア 8 0 に記録されたコンテンツは、記録した機器以外では再生することができないものの、電子配信専用記録メディア 1 2 0 に記録されたコンテンツは、記録した機器以外の機器でも再生することができるようになる。すなわち、通常の記録メディア 8 0 には、コンテンツ鍵  $K_{co}$  で暗号化されたコンテンツがあるだけなので、コンテンツ鍵  $K_{co}$  を持つ（記録した）機器以外では再生ができない。一方、電子配信専用記録メディア 1 2 0 においては、コンテンツ鍵  $K_{co}$  で暗号化されたコンテンツだけでなく、コンテンツ鍵  $K_{co}$  も、電子配信専用記録メディア 1 2 0 個有の保存鍵  $K_{save}$  で暗号化されて保持されているため、他の機器で再生することが可

能になる。

つまり暗号処理部 1 2 2 の相互認証モジュール 1 2 8 と据置機器 5 2 の暗号処理部 7 3 の図示せぬ相互認証モジュール間で相互認証を行った後、専用記録メディア固有の保存鍵  $K_{save3}$  でコンテンツ鍵  $K_{co}$  を復号化し、共有した一時鍵  $K_{temp}$  でコンテンツ鍵  $K_{co}$  を暗号化し、暗号処理部 7 3 へ送信して再生する。

図 1 8 は、各機器内のデータ記憶状況を示すブロック図である。ホームサーバ 5 1 において、暗号処理部 6 5 内の記憶モジュール 9 2 には、機器を特定するための個別 ID (暗号処理部を特定するものと同一)、課金処理する際に使用する決済用 ID (必要に応じて個別 ID で代替できるし、登録情報にあるので不要の場合もある)、機器毎に異なる秘密鍵、保存鍵  $K_{save}$ 、電子配信サービスセンタ 1 と相互認証する際に使用する電子配信サービスセンタ 1 の公開鍵 (電子配信サービスセンタ 1 の公開鍵証明書があれば不要)、公開鍵証明書を検証するための認証局 2 2 の公開鍵、伸張部 6 6 と相互認証する際に使用する共通鍵が記憶されている。これらのデータは、機器製造時に予め記憶されるデータである。これに対し、電子配信サービスセンタ 1 から定期的に配布される配送鍵  $K_d$ 、購入処理の際に書き込まれる課金情報、外部メモリ 6 7 内に保持するコンテンツ鍵  $K_{co}$  および使用許諾条件情報の改竄チェック用のハッシュ値は、機器を使用し始めてから記憶されるデータであり、これらのデータも記憶モジュール 9 2 に記憶されている。伸張部 6 6 内の記憶モジュール 1 0 6 には、伸張部を特定するための個別 ID、暗号処理部 6 5 と相互認証する際に使用する共通鍵が、機器製造時に予め記憶される。なお、暗号処理部 6 5 と伸張部 6 6 を 1 対 1 に対応させるため、それぞれの記憶モジュールに互いの ID を持たせておいても良い (相互認証が共通鍵で行われているため、結果的には対応した暗号処理部、伸張部でしかやりとりができない。但し処理としては公開鍵暗号方式の相互認証であっても良い。このとき保存されている鍵は共通鍵ではなく、伸張部 6 6 固有の秘密鍵になる)。

外部メモリ 6 7 には、コンテンツの復号を行う際に使用する保存鍵  $K_{save}$  で暗号化されたコンテンツ鍵  $K_{co}$ 、そのコンテンツ鍵  $K_{co}$  を利用する際の条件を示す使用



許諾条件情報が記憶されている。また、大容量記憶部 68 には、記憶モジュール 92 内にある機器個別の秘密鍵に対応する公開鍵の証明書（機器の公開鍵証明書）、登録情報、コンテンツプロバイダセキュアコンテナ（コンテンツ鍵  $K_c$  で暗号化されたコンテンツおよびその署名、個別鍵  $K_i$  で暗号化されたコンテンツ鍵  $K_c$  およびその署名、配送鍵  $K_d$  で暗号化された個別鍵  $K_i$  およびその署名、取扱方針およびその署名）、サービスプロバイダセキュアコンテナ（価格情報およびその署名）、コンテンツプロバイダ 2 の公開鍵証明書、サービスプロバイダ 3 の公開鍵証明書が記憶されている。

携帯機器 53 には、ホームサーバ 51 が保持する暗号処理部 65 と同一の暗号処理部 83、外部メモリ 67 と同一の外部メモリ 85 が備えられている（内部データが同一のものは省略されている。例えば、伸張部）。しかし、その内部に保持されるデータは、図に示すように若干異なっている。暗号処理部 83 内の記憶モジュールの保持するデータは、機器を特定するための個別 ID、機器毎に異なる秘密鍵、保存鍵  $K_{save}$ 、電子配信サービスセンタ 1 と相互認証する際に使用する、電子配信サービスセンタ 1 の公開鍵（ただし、ホームサーバ 51 に電子配信サービスセンタ 1 との手続きを全て代行してもらう場合は必要ない）、公開鍵証明書を検証するための認証局 22 の公開鍵、伸張部 84 と相互認証する際に使用する共通鍵が記憶されている。これらのデータは、機器製造時に予め記憶されるデータである。また、外部メモリ 85 内に保持するコンテンツ鍵  $K_c$  および使用許諾条件情報の改竄チェック用のハッシュ値、必要に応じて決済用 ID、配送鍵  $K_d$ 、登録情報（の一部）（購入処理をしない場合、決済用 ID、配送鍵  $K_d$  は必要ない）は、機器を使用し始めてから記憶されるデータであり、これらのデータも記憶されている（購入処理を行う場合、課金情報も記憶される）。外部メモリ 85 には、暗号処理部 83 内にある機器個別の秘密鍵に対応する公開鍵の証明書、コンテンツ鍵  $K_c$  で暗号化されたコンテンツおよびその署名（この他に、必要に応じて個別鍵  $K_i$  で暗号化されたコンテンツ鍵  $K_c$  およびその署名、配送鍵  $K_d$  で暗号化された個別鍵  $K_i$  およびその署名、必要に応じて取扱方針およびその署名、価格

情報およびその署名も記憶される場合がある)、コンテンツを復号化する際に使用する保存鍵 $K_{save}$ で暗号化されたコンテンツ鍵 $K_c$ 、そのコンテンツを利用する際の条件を示す使用許諾条件情報が記憶されている。また、必要に応じてコンテンツプロバイダ2の公開鍵証明書、サービスプロバイダ3の公開鍵証明書も記憶されている。

据置機器52には、ホームサーバ51の構成に加え、記録メディア80が備えられている。記録メディア80としては、通常のMDやCD-Rの場合もあるし、電子配信専用の記憶メディアである場合もある。前者の場合、記憶されるデータはコピー禁止信号を付加された、復号化されたコンテンツになるが、勿論、暗号化されたコンテンツを入れておいてもよい(保存鍵 $K_{save}$ で暗号化されたコンテンツ鍵 $K_c$ も併せて記憶しておいても良い。この時、再生できるのは記憶した機器のみになる。なぜなら、保存鍵 $K_{save}$ は機器毎に異なっているからである)。

また、記憶メディアとしては、図19が考えられる。電子配信専用記憶メディア120において、暗号処理部122内にある記憶モジュール125には、記録メディアの個別ID、記録メディア毎に異なる秘密鍵、この秘密鍵に対応する公開鍵の証明書(外部メモリ123に記録しておいても良い)、コンテンツ鍵 $K_c$ を暗号化するのに使用する保存鍵 $K_{save}$ (一般に、記憶メディア毎に異なる)、電子配信サービスセンタ1の公開鍵(センタとやりとりしない場合や外部メモリ123に電子配信サービスセンタ1の公開鍵証明書が有る場合には必要ない)、認証局の公開鍵、外部メモリ123の改竄を検査するためのハッシュ値、登録情報(の一部)が記憶されている。外部メモリ123には、コンテンツ鍵 $K_c$ で暗号化されたコンテンツ(およびその署名)、保存鍵 $K_{save}$ で暗号化されたコンテンツ鍵 $K_c$ 、使用許諾条件情報が記憶されており、必要に応じて取扱方針(およびその署名)、価格情報(およびその署名)、コンテンツプロバイダ2の公開鍵証明書、サービスプロバイダ3の公開鍵証明書が記憶されている。

図20、図21は、電子配信サービスセンタ1、コンテンツプロバイダ2、サービスプロバイダ3、およびユーザホームネットワーク5の間で送受信される情

報を説明する図である。コンテンツプロバイダ 2 は、コンテンツプロバイダセキュアコンテナ（その詳細は後述する）にコンテンツプロバイダ 2 の公開鍵証明書（その詳細は後述する）を付して、サービスプロバイダ 3 に送信する。また、コンテンツプロバイダ 2 は、必要に応じて取扱方針およびその署名、コンテンツプロバイダ 2 の証明書を電子配信サービスセンタ 1 に送信する。

サービスプロバイダ 3 は、コンテンツプロバイダ 2 の公開鍵証明書を検証し、コンテンツプロバイダ 2 の公開鍵を入手し、受信したコンテンツプロバイダセキュアコンテナの署名を検証する（取扱方針のみ署名検証する場合もある）。署名の検証に成功した後、コンテンツプロバイダセキュアコンテナから取扱方針を取り出し、これを基に価格情報を生成し、価格情報に署名を付けてサービスプロバイダセキュアコンテナとする（その詳細は後述する）。コンテンツプロバイダセキュアコンテナ、サービスプロバイダセキュアコンテナ、コンテンツプロバイダ 2 の公開鍵証明書、およびサービスプロバイダ 3 の公開鍵証明書（その詳細は後述する）をユーザホームネットワーク 5 に送信する。また、サービスプロバイダ 3 は、必要に応じて価格情報およびその署名、サービスプロバイダ 3 の公開鍵証明書を電子配信サービスセンタ 1 に送信する。

ユーザホームネットワーク 5 は、受信したセキュアコンテナを検証した後、セキュアコンテナの中に含まれる取扱方針および価格情報に基づいて購入処理を行い、課金情報を生成して暗号処理部内の記憶モジュールに保存し、使用許諾条件情報を生成し、コンテンツ鍵  $K_{co}$  を復号化して保存鍵  $K_{save}$  で再暗号化し、使用許諾条件情報および再暗号化されたコンテンツ鍵  $K_{co}$  を外部メモリ 6 7 に保存しておく。そして、使用許諾条件情報に沿って、コンテンツ鍵  $K_{co}$  を保存鍵  $K_{save}$  で復号化し、この鍵でコンテンツを復号化して利用する。課金情報は、所定のタイミングで一時鍵  $K_{temp}$  で暗号化され、署名が付され、必要に応じて取扱方針および価格情報と共に電子配信サービスセンタ 1 に送信される。

電子配信サービスセンタ 1 は、課金情報および価格情報を基に使用料金を算出し、また電子配信サービスセンタ 1、コンテンツプロバイダ 2、およびサービス

プロバイダ 3 それぞれの利益を算出する。電子配信サービスセンタ 1 は、さらに、コンテンツプロバイダ 2 から受信した取扱方針、サービスプロバイダ 3 から受信した価格情報、必要に応じて取扱方針、並びにユーザホームネットワーク 5 から受信した取扱方針、価格情報を比較し、サービスプロバイダ 3 またはユーザホームネットワーク 5 で取扱方針の改竄または不正な価格の付加等の不正がなかったか否か等の監視をする。

更に、電子配信サービスセンタ 1 は、コンテンツプロバイダ 2 にコンテンツプロバイダの公開鍵証明書を送信し、サービスプロバイダ 3 にサービスプロバイダの公開鍵証明書を送信する。また、工場出荷時に、各機器に応じて作成した公開鍵証明書を各機器に埋め込むため、各機器の公開鍵証明書に関するデータを工場に引き渡す。

図 2 2 は、コンテンツプロバイダセキュアコンテナを説明する図である。コンテンツプロバイダセキュアコンテナ 1 A は、コンテンツ鍵  $K_{co}$  で暗号化されたコンテンツおよびその署名、個別鍵  $K_i$  で暗号化されたコンテンツ鍵  $K_{co}$  およびその署名、配送鍵  $K_d$  で暗号化された個別鍵  $K_i$  およびその署名、取扱方針および署名を含む。署名は、それぞれのデータにハッシュ関数を適用して生成されたハッシュ値に、コンテンツプロバイダ 2 の秘密鍵  $K_{scp}$  を用いて生成されたデータである。なお、図 2 2 の場合は鍵データ（個別鍵  $K_i$  で暗号化されたコンテンツ鍵  $K_{co}$ 、配送鍵  $K_d$  で暗号化された個別鍵  $K_i$ ）に対してそれぞれ別々に署名を生成し付加するようにしたが、各鍵データ（個別鍵  $K_i$  で暗号化されたコンテンツ鍵  $K_{co}$ 、配送鍵  $K_d$  で暗号化された個別鍵  $K_i$ ）を 1 つにまとめて 1 つの署名を生成し付加するようにしても良い。このように常に一体で使用する鍵データを 1 つにまとめて 1 つの署名を付加することにより、署名の検証が 1 回で済む。

図 2 3 は、コンテンツプロバイダセキュアコンテナの他の例を説明する図である。コンテンツプロバイダセキュアコンテナ 1 B は、コンテンツ鍵  $K_{co}$  で暗号化されたコンテンツおよびその署名、個別鍵  $K_i$  で暗号化されたコンテンツ鍵  $K_{co}$  およびその署名、取扱方針および署名を含む。

図 2 4 は、コンテンツプロバイダセキュアコンテナの他の例を説明する図である。コンテンツプロバイダセキュアコンテナ 1 C は、コンテンツ鍵  $K_{co}$  で暗号化されたコンテンツ、個別鍵  $K_i$  で暗号化されたコンテンツ鍵  $K_{co}$ 、配送鍵  $K_d$  で暗号化された個別鍵  $K_i$ 、取扱方針、および署名を含む。署名は、コンテンツ鍵  $K_{co}$  で暗号化されたコンテンツ、個別鍵  $K_i$  で暗号化されたコンテンツ鍵  $K_{co}$ 、配送鍵  $K_d$  で暗号化された個別鍵  $K_i$ 、および取扱方針にハッシュ関数を適用して生成されたハッシュ値に、コンテンツプロバイダ 2 の秘密鍵  $K_{scp}$  を用いて生成されたデータである。

図 2 5 は、コンテンツプロバイダセキュアコンテナの他の例を説明する図である。コンテンツプロバイダセキュアコンテナ 1 D は、コンテンツ鍵  $K_{co}$  で暗号化されたコンテンツ、個別鍵  $K_i$  で暗号化されたコンテンツ鍵  $K_{co}$ 、取扱方針、および署名を含む。署名は、コンテンツ鍵  $K_{co}$  で暗号化されたコンテンツ、個別鍵  $K_i$  で暗号化されたコンテンツ鍵  $K_{co}$ 、および取扱方針にハッシュ関数を適用して生成されたハッシュ値に、コンテンツプロバイダ 2 の秘密鍵  $K_{scp}$  を用いて生成されたデータである。

図 2 6 は、コンテンツプロバイダ 2 の公開鍵証明書を説明する図である。コンテンツプロバイダ 2 の公開鍵証明書 2 A は、公開鍵証明書のバージョン番号、認証局がコンテンツプロバイダ 2 に対し割り付ける公開鍵証明書の通し番号、署名に用いたアルゴリズムおよびパラメータ、認証局の名前、公開鍵証明書の有効期限、コンテンツプロバイダ 2 の名前、コンテンツプロバイダ 2 の公開鍵  $K_{pcp}$ 、並びに署名を含む。署名は、公開鍵証明書のバージョン番号、認証局がコンテンツプロバイダ 2 に対し割り付ける公開鍵証明書の通し番号、署名に用いたアルゴリズムおよびパラメータ、認証局の名前、公開鍵証明書の有効期限、コンテンツプロバイダ 2 の名前、並びにコンテンツプロバイダ 2 の公開鍵  $K_{pcp}$  にハッシュ関数を適用して生成されたハッシュ値に、認証局の秘密鍵  $K_{sca}$  を用いて生成したデータである。

図 2 7 は、コンテンツプロバイダ 2 の公開鍵証明書の他の例を説明する図であ

る。コンテンツプロバイダ 2 の公開鍵証明書 2 B は、公開鍵証明書のバージョン番号、認証局がコンテンツプロバイダ 2 に対し割り付ける公開鍵証明書の通し番号、署名に用いたアルゴリズムおよびパラメータ、認証局の名前、公開鍵証明書の有効期限、コンテンツプロバイダ 2 の名前、コンテンツプロバイダ 2 の公開鍵  $K_{pcp}$ 、配送鍵  $K_d$  で暗号化された個別鍵  $K_i$ 、並びに署名を含む。署名は、公開鍵証明書のバージョン番号、認証局がコンテンツプロバイダ 2 に対し割り付ける公開鍵証明書の通し番号、署名に用いたアルゴリズムおよびパラメータ、認証局の名前、公開鍵証明書の有効期限、コンテンツプロバイダ 2 の名前、コンテンツプロバイダ 2 の公開鍵  $K_{pcp}$ 、並びに配送鍵  $K_d$  で暗号化された個別鍵  $K_i$  にハッシュ関数を適用して生成されたハッシュ値に、認証局の秘密鍵  $K_{sca}$  を用いて生成したデータである。

図 28 は、コンテンツプロバイダ 2 の公開鍵証明書のまた別の例を説明する図である。コンテンツプロバイダ 2 の公開鍵証明書 2 C は、公開鍵証明書のバージョン番号、認証局がコンテンツプロバイダ 2 に対し割り付ける公開鍵証明書の通し番号、署名に用いたアルゴリズムおよびパラメータ、認証局の名前、公開鍵証明書の有効期限、コンテンツプロバイダ 2 の名前、コンテンツプロバイダ 2 の公開鍵  $K_{pcp}$ 、個別鍵  $K_i$  の一部を配送鍵  $K_d$  で暗号化した、所定の種類のデータ、並びに署名を含む。署名は、公開鍵証明書のバージョン番号、認証局がコンテンツプロバイダ 2 に対し割り付ける公開鍵証明書の通し番号、署名に用いたアルゴリズムおよびパラメータ、認証局の名前、公開鍵証明書の有効期限、コンテンツプロバイダ 2 の名前、コンテンツプロバイダ 2 の公開鍵  $K_{pcp}$ 、並びに個別鍵  $K_i$  の一部を配送鍵  $K_d$  で暗号化した、所定の種類のデータにハッシュ関数を適用して生成されたハッシュ値に、認証局の秘密鍵  $K_{sca}$  を用いて生成したデータである。

図 29 は、サービスプロバイダセキュアコンテナを説明する図である。サービスプロバイダセキュアコンテナ 3 A は、価格情報および署名で構成されている。署名は、価格情報に対し必要に応じてハッシュ関数を適用して生成されたハッシュ値に、サービスプロバイダ 3 の秘密鍵  $K_{ssp}$  を用いて生成されたデータである。

図30は、サービスプロバイダセキュアコンテナの他の例を説明する図である。サービスプロバイダセキュアコンテナ3Bは、コンテンツプロバイダセキュアコンテナ、価格情報、および署名を含む。署名は、コンテンツプロバイダセキュアコンテナ、および価格情報にハッシュ関数を適用して生成されたハッシュ値に、サービスプロバイダ3の秘密鍵 $K_{ssp}$ を用いて生成されたデータである。

図31は、サービスプロバイダ3の公開鍵証明書を説明する図である。サービスプロバイダ3の公開鍵証明書4Aは、公開鍵証明書のバージョン番号、認証局がサービスプロバイダ3に対し割り付ける公開鍵証明書の通し番号、署名に用いたアルゴリズムおよびパラメータ、認証局の名前、公開鍵証明書の有効期限、サービスプロバイダ3の名前、サービスプロバイダ3の公開鍵 $K_{psp}$ 、並びに署名を含む。署名は、公開鍵証明書のバージョン番号、認証局がサービスプロバイダ3に対し割り付ける公開鍵証明書の通し番号、署名に用いたアルゴリズムおよびパラメータ、認証局の名前、公開鍵証明書の有効期限、サービスプロバイダ3の名前、並びにサービスプロバイダ3の公開鍵 $K_{psp}$ にハッシュ関数を適用して生成されたハッシュ値に、認証局の秘密鍵 $K_{sca}$ を用いて生成したデータである。

図32は、User機器の公開鍵証明書を説明する図である。User機器の公開鍵証明書5Aは、公開鍵証明書のバージョン番号、認証局がUser機器（正確には暗号処理部（専用のICチップ））に対し割り付ける公開鍵証明書の通し番号、署名に用いたアルゴリズムおよびパラメータ、認証局の名前、公開鍵証明書の有効期限、User機器の名前、User機器の公開鍵 $K_{pu}$ 、並びに署名を含む。署名は、公開鍵証明書のバージョン番号、認証局がUser機器に対し割り付ける公開鍵証明書の通し番号、署名に用いたアルゴリズムおよびパラメータ、認証局の名前、公開鍵証明書の有効期限、User機器の名前、並びにUser機器の公開鍵 $K_{pu}$ にハッシュ関数を適用して生成されたハッシュ値に、認証局の秘密鍵 $K_{sca}$ を用いて生成したデータである。

図33および図34は取扱方針のデータフォーマットを示すものであり、当該取扱方針はコンテンツプロバイダ2によりシングルコンテンツ毎、またアルバム

コンテンツ毎に生成され、ユーザホームネットワーク 5 が購入可能な利用権の内容を示す。

シングルコンテンツに対する取扱方針（図 3 3）のデータには、データの種別、取扱方針の種類、取扱方針の有効期限、コンテンツの ID、コンテンツプロバイダの ID、取扱方針の ID、取扱方針のバージョン、地域コード、使用可能機器条件、使用可能 User 条件、サービスプロバイダの ID、世代管理情報、当該取扱方針が示す購入可能な利用権を含むルールの数、当該ルールの格納位置を示すアドレス情報、そのアドレス情報の示す位置に格納されたルール、公開鍵証明書、署名が格納されている。

そして、ルールは、利用権毎に整理番号として付けられたルール番号、利用権内容を示す利用権内容番号、そのパラメータ、最低販売価格、コンテンツプロバイダの利益額、当該コンテンツプロバイダの利益率、データサイズ、送信情報から構成されている。

また、アルバムコンテンツに対する取扱方針（図 3 4）のデータには、データの種別、取扱方針の種類、取扱方針の有効期限、アルバムの ID、取扱方針のバージョン、コンテンツプロバイダの ID、取扱方針の ID、地域コード、使用可能機器条件、使用可能 User 条件、サービスプロバイダの ID、当該アルバムを構成するシングルコンテンツの取扱方針の数、そのシングルコンテンツの取扱方針の格納位置を示すアドレス情報、当該アドレス情報の示す位置に格納されたシングルコンテンツの取扱方針のデータパケット、世代管理情報、当該取扱方針が示す購入可能な利用権を含むルールの数、当該ルールの格納位置を示すアドレス情報、そのアドレス情報の示す位置に格納されたルール、公開鍵証明書、署名が格納されている。

そして、ルールは、シングルコンテンツの取扱方針のルールと同様に、利用権毎に整理番号として付けられたルール番号、利用権内容番号、パラメータ、最低販売価格、コンテンツプロバイダの利益額、当該コンテンツプロバイダの利益率、データサイズ、送信情報から構成されている。



これら取扱方針において、データの種別はそのデータが取扱方針のデータであることを示し、取扱方針の種類は当該取扱方針がシングル又はアルバムコンテンツのいずれの取扱方針であるかを示している。取扱方針の有効期限は当該取扱方針の使用期間をその期限の切れる日付、又は使用を開始した基準となる日から期限の切れる日までの日数などによって示している。コンテンツのIDおよびアルバムのIDは取扱方針が示す購入可能なシングルコンテンツおよびアルバムコンテンツを示し、コンテンツプロバイダのIDは、当該取扱方針を規定したコンテンツプロバイダ2のIDを示している。

また、取扱方針のIDは当該取扱方針を識別するためのものであり、例えば、同一コンテンツに対して複数の取扱方針が設定された場合などに当該取扱方針を識別するために使用される。取扱方針のバージョンは使用期間に応じて改訂した取扱方針のその改訂情報を示している。従って、取扱方針はこれら取扱方針のIDおよび取扱方針のバージョンにより管理される。

地域コードは取扱方針の使用可能な地域をコード化して示しており、当該地域コードには取扱方針の使用可能な地域を限定する特定の地域を示すコードと、当該取扱方針を全ての地域で使用可能にするコードを割り当てることができる。使用可能機器条件は取扱方針を利用し得る機器の条件を示し、使用可能User条件は取扱方針を利用し得るユーザの条件を示している。

サービスプロバイダのIDは取扱方針を利用するサービスプロバイダ3のIDを示しており、当該サービスプロバイダのIDには取扱方針を使用し得るサービスプロバイダ3を限定する特定のサービスプロバイダ3のIDと、当該取扱方針を複数（全て）のサービスプロバイダで使用し得るようにするIDとがある。

さらに、世代管理情報はコンテンツの再購入可能な最大回数を示す。署名は取扱方針から当該署名を除く、データの種別から公開鍵証明書までの全体に対して付けられるものである。署名を作成する際に用いたアルゴリズムおよびパラメータと、当該署名の検証に用いる鍵は公開鍵証明書に含まれている。

また、ルールにおいて、利用権内容番号は、利用権内容毎に付加された番号で

あり、パラメータは権利内容のパラメータを示す。最低販売価格は利用権内容に応じてシングルおよびアルバムコンテンツを販売する際の最低の販売価格を示し、コンテンツプロバイダの利益額および利益率はシングルコンテンツおよびアルバムコンテンツが購入されたときにコンテンツプロバイダ2が得ることのできる利益の金額および販売価格に対する利益率を示している。データサイズは送信情報のデータサイズを示し、当該送信情報は、コンテンツプロバイダ2が設定した、利用権の購入によりユーザに加算されるポイントや、当該ポイントに応じた利用権の割引額となるマイル情報や、必要に応じてコンテンツプロバイダ2が設定した各種情報からなる。

ここで、アルバムコンテンツの取扱方針において、複数のルールは、当該アルバムの購入形態を示している。また、アルバムコンテンツの取扱方針に格納された複数のシングルコンテンツの取扱方針において、当該取扱方針に格納されたルールは、それぞれ対応するシングルコンテンツがアルバムのなかから、シングル曲として単独で購入し得る、又は対応するシングルコンテンツがアルバム曲としてのみ購入し得る（すなわち、アルバムとして、他のシングルコンテンツと共に一体化してしか購入し得ない）等のようにアルバム内におけるシングルコンテンツの購入形態を示している。

従って、アルバムコンテンツの取扱方針においては、当該取扱方針のルールに基づいて、アルバムコンテンツを購入し、又はシングルコンテンツの取扱方針のルールに基づいて、シングルコンテンツをシングル曲として購入するように、アルバムコンテンツと、シングル曲として販売し得るシングルコンテンツとのいずれも選択して購入し得るように定義されている。

また、アルバムコンテンツの取扱方針においては、全体に対して署名を付けたことにより、当該署名を検証するだけで、この取扱方針に格納したシングルコンテンツの取扱方針の署名をそれぞれ検証しなくてもこのアルバムコンテンツの取扱方針と共に、各シングルコンテンツの取扱方針に対しても合わせて改竄のチェックなどを行うことができ、かくして署名の検証を簡易化し得る。

因みに、シングルおよびアルバムコンテンツの取扱方針には、必要に応じて、コンテンツに対する署名の検証を実行するか否かを示す署名の検証の有無を格納し得る。これは、コンテンツのデータ量が比較的多く、署名の検証に時間がかかるためであり、取扱方針にかかる署名の検証の有無の情報が格納された場合には、当該情報に従ってコンテンツの署名の検証を実行し、又は当該検証を実行しないようにする。

また、アルバムコンテンツの取扱方針においては、当該アルバムを構成する複数のシングルコンテンツの取扱方針を格納しているものの、これら複数のシングルコンテンツの取扱方針を格納しなくても良い。

さらに、シングルおよびアルバムコンテンツの取扱方針においては、コンテンツプロバイダの利益額および利益率を電子配信サービスセンタ 1 により一括管理しても良いため、図 3 5 および図 3 6 に示すように、これらコンテンツプロバイダの利益額および利益率を除いて構成しても良い。

図 3 7 および図 3 8 は価格情報のデータフォーマットを示すものであり、当該価格情報はサービスプロバイダ 3 において、コンテンツプロバイダ 2 から与えられるシングルコンテンツの取扱方針毎、またアルバムコンテンツの取扱方針毎に生成され、シングルコンテンツおよびアルバムコンテンツの価格を示す。

シングルコンテンツに対する価格情報（図 3 7）のデータには、データの種別、価格情報の種類、価格情報の有効期限、コンテンツの ID、サービスプロバイダの ID、価格情報の ID、価格情報のバージョン、地域コード、使用可能機器条件、使用可能 User 条件、コンテンツプロバイダの ID、当該価格情報が付加された取扱方針の ID、当該価格情報が示す購入可能な利用権を含むルールの数、当該ルールの格納位置を示すアドレス情報、そのアドレス情報の示す位置に格納されたルール、公開鍵証明書、署名が格納されている。

そして、ルールは利用権毎に整理番号として付けられたルール番号、サービスプロバイダの利益額、当該サービスプロバイダの利益率、価格、データサイズ、送信情報から構成されている。

また、アルバムコンテンツに対する価格情報（図38）のデータには、データの種別、価格情報の種類、価格情報の有効期限、アルバムのID、サービスプロバイダのID、価格情報のID、価格情報のバージョン、地域コード、使用可能機器条件、使用可能User条件、コンテンツプロバイダのID、当該価格情報が付加された取扱方針のID、当該アルバムを構成するシングルコンテンツの価格情報の数、そのシングルコンテンツの価格情報の格納位置を示すアドレス情報、当該アドレス情報の示す位置に格納されたシングルコンテンツの価格情報のデータパケット、当該価格情報が示す購入可能な利用権を含むルールの数、そのルールの格納位置を示すアドレス情報、当該アドレス情報の示す位置に格納されたルール、公開鍵証明書、署名が格納されている。

そして、ルールは、シングルコンテンツに対する価格情報のルールと同様に、利用権毎に整理番号として付けられたルール番号、サービスプロバイダの利益額、当該サービスプロバイダの利益率、価格、データサイズ、送信情報から構成されている。

これら価格情報において、データの種別はこのデータが価格情報のデータであることを示し、価格情報の種類は当該価格情報がシングルコンテンツ又はアルバムコンテンツのいずれの価格情報であるかを示している。価格情報の有効期限は当該価格情報の使用期間をその期限の切れる日付、又は使用開始の基準となる日から期限の切れる日までの日数などによって示している。コンテンツのIDおよびアルバムのIDは価格情報が示す購入可能なシングルコンテンツおよびアルバムコンテンツを示し、サービスプロバイダのIDは当該価格情報を作成したサービスプロバイダ3のIDを示している。

また、価格情報のIDは当該価格情報を識別するためのものであり、例えば、同一コンテンツに対して複数の価格情報が設定された場合などに当該価格情報を識別するために使用される。価格情報のバージョンは使用期間に応じて改訂された価格情報の改訂情報を示している。従って、価格情報はこれら価格情報のIDおよび価格情報のバージョンにより管理される。

地域コードは価格情報の使用可能な地域をコード化して示しており、当該地域コードには価格情報の使用可能な地域を限定する特定の地域を示すコードと、当該価格情報を全ての地域で使用可能にするコードを割り当てることができる。使用可能機器条件は価格情報を利用し得る機器の条件を示し、使用可能User条件は価格情報を利用し得るユーザの条件を示している。コンテンツプロバイダのIDは価格情報を付加した取扱方針を規定したコンテンツプロバイダ2のIDを示している。取扱方針のIDは価格情報を付加した取扱方針を識別するためのものである。

さらに、署名は価格情報から当該署名を除く、データの種別から公開鍵証明書までの全体に対して付けられるものである。署名を作成する際に用いたアルゴリズムおよびパラメータと、当該署名の検証に用いる鍵は公開鍵証明書に含まれている。

また、ルールにおいて、ルール番号は対応する取扱方針が示すルールのルール番号をそのまま用いる。サービスプロバイダの利益額および利益率はシングルコンテンツおよびアルバムコンテンツが購入されたときにサービスプロバイダ3が得ることのできる利益の金額および価格に対する利益率を示し、価格はサービスプロバイダ3により利用権内容および対応する最低販売価格に基づいて設定されたシングルコンテンツおよびアルバムコンテンツの販売価格を示す。データサイズは送信情報のデータサイズを示し、当該送信情報は、サービスプロバイダ3が設定した、利用権の購入によりユーザに加算されるポイントや、当該ポイントに応じた利用権の割引額となるマイル情報や、必要に応じてサービスプロバイダ3が設定した各種情報からなる。

ここで、サービスプロバイダ3は、価格情報を生成する際、対応する取扱方針が示す購入可能な全ての利用権を当該価格情報が示す購入可能な利用権として設定できると共に、当該取扱方針が示す購入可能な全ての利用権のうちから任意に選定した利用権を価格情報が示す購入可能な利用権として設定することもでき、コンテンツプロバイダ2が規定した利用権を選定し得る。

また、アルバムコンテンツの価格情報において、複数のルールは、アルバムの購入形態に応じた販売価格を規定している。また、アルバムコンテンツの価格情報に格納された複数のシングルコンテンツの価格情報のうち、シングル曲として販売し得るシングルコンテンツの価格情報のルールは、当該シングル曲として販売し得るシングルコンテンツの販売価格を規定している。

従って、アルバムコンテンツの価格情報においては、当該価格情報1つでアルバムの販売価格と、シングル曲として販売し得るシングルコンテンツの販売価格とを認識し得るようになされている。

また、アルバムコンテンツの価格情報においては、全体に対して署名を付けたことにより、当該署名を検証するだけで、この価格情報に格納したシングルコンテンツの価格情報の署名をそれぞれ検証しなくてもこのアルバムコンテンツの価格情報と共に、各シングルコンテンツの価格情報に対しても合わせて改竄のチェックなどを行うことができ、かくして署名の検証を簡易化し得る。

因みに、シングルおよびアルバムの価格情報においては、図33および図34について上述した取扱方針と同様にコンテンツに対する署名の検証の有無を格納し得る。また、アルバムコンテンツの価格情報においては、当該アルバムを構成する複数のシングルコンテンツの価格情報を格納しているものの、これら複数のシングルコンテンツの価格情報を格納しなくても良い。

さらに、シングルおよびアルバムコンテンツの価格情報においては、サービスプロバイダの利益額および利益率を電子配信サービスセンタ1により一括管理しても良いため、図39および図40に示すように、これらサービスプロバイダの利益額および利益率を除いて構成しても良い。

図41は使用許諾条件情報のデータフォーマットを示すものであり、当該使用許諾条件情報はユーザホームネットワーク5内の機器において、ユーザがコンテンツを購入した際、当該購入したコンテンツの取扱方針に基づいて作成され、この取扱方針の示す利用権内容のうちのユーザが選択した利用権内容を示す。

使用許諾条件情報のデータには、データの種別、使用許諾条件情報の種類、使

用許諾条件情報の有効期限、コンテンツのID、アルバムのID、暗号処理部のID、ユーザのID、コンテンツプロバイダのID、取扱方針のID、取扱方針のバージョン、サービスプロバイダのID、価格情報のID、価格情報のバージョン、使用許諾条件情報のID、再生権（利用権）に整理番号として付けられたルール番号、利用権内容番号、再生残り回数、再生権の有効期限、複製権（利用権）に整理番号として付けられたルール番号、利用権内容番号、複製の残り回数、世代管理情報、再生権を保有する暗号処理部のIDが格納されている。

使用許諾条件情報において、データの種別はこのデータが使用許諾条件情報のデータであることを示し、使用許諾条件情報の種類は当該使用許諾条件情報がシングルコンテンツ又はアルバムコンテンツのいずれの使用許諾条件情報であることを示している。使用許諾条件情報の有効期限は当該使用許諾条件情報の使用期間をその期限の切れる日付、又は使用開始の基準となる日から期限の切れる日までの日数などによって示している。

コンテンツのIDには購入されたシングルコンテンツを示すIDが記述され、アルバムのIDにはアルバムが購入されたときのみ当該アルバムを示すIDが記述される。実際には、コンテンツがシングルとして購入された場合、コンテンツのIDのみに購入されたシングルコンテンツを示すIDが記述され、また、コンテンツがアルバムとして購入された場合には、コンテンツのIDに、アルバムを構成する全てのシングルコンテンツのIDが記述され、かつアルバムのIDに購入されたアルバムを示すIDが記述される。従って、このアルバムのIDをみれば、購入されたコンテンツがシングルであるか、又はアルバムであるかを容易に判断し得る。

暗号処理部のIDはコンテンツを購入処理したユーザホームネットワーク5内の機器の暗号処理部を示す。ユーザのIDはコンテンツを購入したユーザホームネットワーク5内の機器を複数のユーザが共有しているときに、当該機器を共有する複数のユーザを示している。

また、コンテンツプロバイダのIDは使用許諾条件情報を作成するために用い

た取扱方針を規定したコンテンツプロバイダ 2 の ID を示し、取扱方針の ID は当該使用許諾条件情報を作成するために用いた取扱方針を示す。取扱方針のバージョンは使用許諾条件情報を作成するために用いた取扱方針の改訂情報を示している。サービスプロバイダの ID は使用許諾条件情報を作成するために用いた価格情報を作成したサービスプロバイダ 3 の ID を示し、価格情報の ID は当該使用許諾条件情報を作成するために用いた価格情報を示す。価格情報のバージョンは使用許諾条件情報を作成するために用いた取扱方針の改訂情報を示している。従って、これらコンテンツプロバイダの ID、取扱方針の ID、取扱方針のバージョン、サービスプロバイダの ID、価格情報の ID および価格情報のバージョンにより、ユーザが購入したコンテンツを提供したコンテンツプロバイダ 2 又はサービスプロバイダ 3 を知り得るようになされている。

使用許諾条件情報の ID はコンテンツを購入したユーザホームネットワーク 5 内の機器の暗号処理部が付けるものであり、当該使用許諾条件情報を識別するために使用される。再生権のルール番号は利用権のうちの再生権に付けられた整理番号を示し、対応する取扱方針および価格情報が示すルールのルール番号をそのまま用いる。利用権内容は後述する再生権の内容を示す。再生残り回数は購入したコンテンツに対して予め設定された再生回数のうちの残りの再生回数を示し、再生権の有効期限は購入したコンテンツの対する再生可能期間をその期限の切れる日時などによって示している。

また、複製権のルール番号は利用権のうちの複製権に付けられた整理番号を示し、対応する取扱方針および価格情報が示すルールのルール番号をそのまま用いる。利用権内容は後述する複製権の内容を示す。複製残り回数は購入したコンテンツに対して予め設定された複製回数のうちの残りの複製回数を示す。

さらに、世代管理情報はコンテンツを再購入した際に当該コンテンツの再購入可能な残り回数を示す。再生権を保有する暗号処理部の ID は現時点において再生権を保有する暗号処理部を示しており、管理移動したときには再生権を保有する暗号処理部の ID が変更される。



因みに、使用許諾条件情報においては、複製権に対して有効期限を規定しても良く、当該有効期限を規定した場合には購入したコンテンツの対する複製可能期間をその期限の切れる日時などによって示す。

図 4 2 は課金情報を示すものであり、当該課金情報はユーザホームネットワーク 5 内の機器により、コンテンツの購入の際に、当該コンテンツに対応する取扱方針および価格情報に基づいて生成される。

課金情報のデータには、データの種別、暗号処理部の ID、ユーザの ID、コンテンツの ID、コンテンツプロバイダの ID、取扱方針の ID、取扱方針のバージョン、サービスプロバイダの ID、価格情報の ID、価格情報のバージョン、使用許諾条件情報の ID、ルール番号、コンテンツプロバイダ 2 の利益額および利益率、サービスプロバイダの利益額および利益率、世代管理情報、コンテンツプロバイダの設定した送信情報のデータサイズ、そのコンテンツプロバイダの設定した送信情報、サービスプロバイダの設定した送信情報のデータサイズ、そのサービスプロバイダの設定した送信情報、供給元の ID が格納されている。

課金情報において、データの種別は当該データが課金情報であることを示し、暗号処理部の ID は、コンテンツの購入処理を実行して当該課金情報を生成した機器の暗号処理部を示す。ユーザの ID はコンテンツを購入したユーザホームネットワーク 5 内の機器を複数のユーザが共有しているときに、当該機器を共有する複数のユーザを示し、コンテンツの ID は当該購入されたコンテンツ（シングルコンテンツ又はアルバムコンテンツ）を示す。

また、コンテンツプロバイダの ID は購入処理に用いた取扱方針を規定したコンテンツプロバイダ 2 の ID（この取扱方針に含まれるコンテンツプロバイダの ID）を示し、取扱方針の ID は当該購入処理に用いた取扱方針を示す。取扱方針のバージョンは、購入処理に用いた取扱方針の改訂情報を示す。サービスプロバイダの ID は購入処理に用いた価格情報を作成したサービスプロバイダ 3 の ID（この価格情報に含まれるサービスプロバイダの ID）を示し、価格情報の ID は当該購入処理に用いた価格情報を示す。価格情報のバージョンは、購入処理

に用いた価格情報の改訂情報を示す。

使用許諾条件情報の I D は購入処理の際に作成した使用許諾条件情報の I D を示し、ルール番号は購入された利用権に整理番号として付けられたルール番号を示す。コンテンツプロバイダの利益額および利益率はコンテンツの購入によりコンテンツプロバイダ 2 に分配される配当の金額および売上に対する割合を示し、サービスプロバイダの利益額および利益率は当該コンテンツの購入によりサービスプロバイダ 3 に分配される配当の金額および売上に対する割合を示す。

さらに、世代管理情報は購入されたコンテンツの世代を示す。また、コンテンツプロバイダの設定した送信情報のデータサイズおよびそのコンテンツプロバイダの設定した送信情報には、購入処理に用いた取扱方針が示すデータサイズと、送信情報をそのまま格納すると共に、サービスプロバイダの設定した送信情報のデータサイズおよびそのサービスプロバイダの設定した送信情報には購入処理に用いた価格情報が示すデータサイズと、送信情報をそのまま格納する。そして、供給元の I D は、購入処理したコンテンツの供給元の機器を示し、この I D はコンテンツの再購入が行われる毎に累積される。

因みに、課金情報においては、コンテンツプロバイダの利益額および利益率と、サービスプロバイダの利益額および利益率を電子配信サービスセンタ 1 により一括管理しても良いため、図 4 3 に示すように、これらコンテンツプロバイダの利益額および利益率およびサービスプロバイダの利益額および利益率を除いて構成しても良い。

図 4 4 は購入可能な利用権の内容を示したものであり、当該利用権としては、大きく分けて再生権、複製権、権利内容変更権、再購入権、追加購入権、管理移動権がある。

再生権には、期間制限および回数制限のない無制限再生権と、再生期間を制限する期間制限付き再生権、再生の積算時間を制限する積算時間制限付き再生権、再生回数を制限する回数制限付き再生権がある。複製権には、期間制限、回数制限およびコピー管理情報（例えば、シリアルコピーマネージメント：SCMS）

のないコピー管理情報なし無制限複製権、複製回数を制限するもののコピー管理情報のない回数制限付きおよびコピー管理情報なし複製権、期間制限および回数制限はないもののコピー管理情報を付加して提供するコピー管理情報付き複製権、複製回数を制限し、かつコピー管理情報を付加して提供する回数制限およびコピー管理情報付き複製権がある。因みに、複製権としては、この他に複製可能期間を制限する期間制限付き複製権（コピー管理情報を付加するものと、当該コピー管理情報を付加しないものがある）や、複製の積算時間（すなわち、複製されたコンテンツの再生に要する積算時間）を制限する積算時間制限付き複製権（コピー管理情報を付加するものと、当該コピー管理情報を付加しないものがある）等がある。

また、権利内容変更権は上述したように既に購入した利用権の内容を別の内容に変更する権利であり、再購入権も上述したように他の機器で購入した権利に基づき利用権を別途購入する権利である。追加購入権は、既に単独で購入したコンテンツに当該コンテンツを含むアルバムの他のコンテンツを追加購入してアルバム化する権利であり、管理移動権は購入した利用権を移動して保有者を変更する権利である。

次に、図 3 3 などに示されている利用権内容の具体例を説明する。実際に、無制限再生権のデータとしては、図 4 5 A に示すように、再生権の有効期間をその期限の切れる日付、又は有効期間開始の基準となる日から期限の切れる日までの日数などによって示す当該再生権の有効期限の情報が利用権内容の領域に格納される。期間制限付き再生権のデータとしては、図 4 5 B に示すように、再生権の有効期間をその期限の切れる日付、又は有効期間開始の基準となる日から期限の切れる日までの日数などによって示す当該再生権の有効期限の情報が利用権内容の領域に格納される。

積算時間制限付き再生権のデータとしては、図 4 5 C に示すように再生権の有効期間をその期限の切れる日付、又は有効期間開始の基準となる日から期限の切れる日までの日数などによって示す当該再生権の有効期限の情報と、再生し得る

積算時間の制限を示す日数および時間の情報とが利用権内容の領域に格納される。回数制限付き再生権のデータとしては、図 4 5 D に示すように、再生権の有効期間をその期限の切れる日付、又は有効期間開始の基準となる日から期限の切れる日までの日数などによって示す当該再生権の有効期限の情報と、再生し得る回数を示す再生回数の情報とが利用権内容の領域に格納される。

また、コピー管理情報なし無制限複製権のデータとしては、図 4 5 E に示すように、複製権の有効期間をその期限の切れる日付、又は有効期間開始の基準となる日から期限の切れる日までの日数などによって示す当該複製権の有効期限の情報が利用権内容の領域に格納されている。回数制限付きおよびコピー管理情報なし複製権のデータとしては、図 4 5 F に示すように、複製権の有効期間をその期限の切れる日付、又は有効期間開始の基準となる日から期限の切れる日までの日数などによって示す当該複製権の有効期限の情報と、複製し得る回数を示す複製回数の情報とが利用権内容の領域に格納される。

コピー管理情報付き複製権のデータとしては、図 4 5 G に示すように、複製権の有効期間をその期限の切れる日付、又は有効期間開始の基準となる日から期限の切れる日までの日数などによって示す当該複製権の有効期限の情報が利用権内容の領域に格納されている。回数制限およびコピー管理情報付き複製権のデータとしては、図 4 5 H に示すように、複製権の有効期間をその期限の切れる日付、又は有効期間開始の基準となる日から期限の切れる日までの日数などによって示す当該複製権の有効期限の情報と、複製し得る回数を示す複製回数の情報とが利用権内容の領域に格納される。

さらに、権利内容変更権のデータとしては、図 4 5 I に示すように、当該権利内容変更権の有効期間をその期限の切れる日付、又は有効期間開始の基準となる日から期限の切れる日までの日数などによって示す当該権利内容変更権の有効期限の情報と、変更前の利用権内容を検索するための旧ルール番号と、変更後の利用権内容を検索するための新ルール番号とが利用権内容の領域に格納される。因みに、利用権内容として、例えば、期間制限付き再生権 1 つをみても、その期間

の設定により複数種類の期間制限付き再生権が存在するように、利用権内容毎に複数種類の内容が存在する。従って、利用権内容を利用権内容番号だけでは管理し難いため、権利内容変更権においては、これら利用権内容毎の複数の内容毎に付けられたルール番号により利用権内容を管理する。

再購入権のデータとしては、図 4 5 J に示すように、当該再購入権の有効期間をその期限の切れる日付、又は有効期間開始の基準となる日から期限の切れる日までの日数などによって示す当該再購入権の有効期限の情報と、再購入前の利用権内容を検索するための旧ルール番号と、再購入後の利用権内容を検索するための新ルール番号と、再購入し得る最大回数の示す最大配信世代情報とが利用権内容の領域に格納される。

追加購入権のデータとしては、図 4 5 K に示すように、当該追加購入権の有効期間をその期限の切れる日付、又は有効期間開始の基準となる日から期限の切れる日までの日数などによって示す当該追加購入権の有効期限の情報と、アルバムコンテンツを構成する複数のシングルコンテンツのうちの既に購入したシングルのコンテンツを示す最小保有コンテンツ数および最大保有コンテンツ数とが利用権内容の領域に格納される。

管理移動権のデータとしては、図 4 5 L に示すように、当該管理移動権の有効期間をその期限の切れる日付、又は有効期間開始の基準となる日から期限の切れる日までの日数などによって示す当該管理移動権の有効期限の情報が利用権内容の領域に格納される。

因みに、かかる利用権内容として、例えば、ゲームのデータを複数のコンテンツに分割した際にこれらコンテンツを所定の順番に従って購入するためのコンテンツ購入権を規定しても良い。そして、コンテンツ購入権のデータとしては、図 4 5 M に示すように、当該コンテンツ購入権の有効期間をその期限の切れる日付、又は有効期間開始の基準となる日から期限の切れる日までの日数などによって示す当該コンテンツ購入権の有効期限の情報と、既に購入されているコンテンツの ID と、既に購入された利用権内容を検索するための旧ルール番号と、新たに

購入する利用権内容を検索するための新ルール番号とを利用権内容の領域に格納する。このようにすることで、連続したストーリーをもつゲームプログラムなどを、ユーザに連続して購入させるようにしたり、また、コンテンツ（ゲーム）そのものをアップグレードし得る。

図46はシングルコンテンツのデータフォーマットを示すものであり、当該シングルコンテンツのデータには、データの種別、コンテンツの種類、コンテンツの有効期限、コンテンツのカテゴリ、コンテンツのID、コンテンツプロバイダのID、コンテンツの暗号方式、暗号化したコンテンツのデータ長、その暗号化したコンテンツ、公開鍵証明書、署名が格納されている。

このシングルコンテンツにおいて、データの種別はそのデータがコンテンツのデータであることを示し、コンテンツの種類は当該コンテンツがシングルであることを示す。コンテンツの有効期限は当該コンテンツの配信期限をこの期限の切れる日付、又は配信を開始した基準となる日から期限の切れる日までの日数などによって示している。コンテンツのカテゴリは当該コンテンツが音楽データ、プログラムデータ、映像データなどのいずれのカテゴリのものであるかを示し、コンテンツのIDはこのシングルコンテンツを識別するためのものである。

コンテンツプロバイダのIDは、このシングルコンテンツを保有するコンテンツプロバイダ2のIDを示す。コンテンツの暗号方式は当該コンテンツの暗号に用いる暗号方式（例えば、DES）を示す。署名はシングルコンテンツのデータから当該署名を除く、データの種別から公開鍵証明書までの全体に対して付けられるものである。署名を作成する際に用いたアルゴリズムおよびパラメータと、当該署名の検証に用いる鍵は公開鍵証明書に含まれている。

また、図47はアルバムコンテンツのデータフォーマットを示すものであり、当該アルバムコンテンツのデータには、データの種別、コンテンツの種類、コンテンツの有効期限、アルバムのID、コンテンツプロバイダのID、シングルコンテンツの数、シングルコンテンツのアドレス情報、シングルコンテンツ、公開鍵証明書、署名が格納されている。

このアルバムコンテンツにおいて、データの種別はそのデータがコンテンツのデータであることを示し、コンテンツの種類は当該コンテンツがアルバムであることを示す。コンテンツの有効期限は当該コンテンツの配信期限をこの期限の切れる日付、又は配信を開始した基準となる日から期限の切れる日までの日数などによって示し、アルバムのIDはこのアルバムコンテンツを識別するためのものである。

コンテンツプロバイダのIDは、このアルバムコンテンツを保有するコンテンツプロバイダ2のIDを示す。シングルコンテンツの数はアルバムを構成するシングルコンテンツの数を示し、シングルコンテンツのアドレス情報は当該アルバムを構成するシングルコンテンツの格納位置を示し、そして、シングルコンテンツは当該アドレス情報の示す位置に実際に格納された、このアルバムを構成する複数のシングルコンテンツのデータパケットである。また、署名はアルバムコンテンツのデータから当該署名を除く、データの種別から公開鍵証明書までの全体に対して付けられるものである。署名を作成する際に用いたアルゴリズムおよびパラメータと、当該署名の検証に用いる鍵は公開鍵証明書に含まれている。

そして、アルバムコンテンツにおいては、全体に対して署名を付けたことにより、当該署名を検証するだけで、このアルバムコンテンツに格納したシングルコンテンツの署名をそれぞれ検証しなくても当該アルバムコンテンツと共に、各シングルコンテンツに対しても合わせて改竄のチェックなどを行うことができ、かくして署名の検証を簡易化し得る。

図48はシングルコンテンツ用の鍵のデータフォーマットを示すものであり、当該シングルコンテンツ用の鍵データには、データの種別、鍵データの種類、鍵の有効期限、コンテンツのID、コンテンツプロバイダのID、鍵のバージョン、コンテンツ鍵 $K_c$ の暗号方式、暗号化されたコンテンツ鍵 $K_c$ 、個別鍵 $K_i$ の暗号方式、暗号化された個別鍵 $K_i$ 、公開鍵証明書、署名が格納されている。

シングルコンテンツ用の鍵データにおいて、データの種別はこのデータが鍵のデータであることを示し、鍵データの種類は当該鍵データがシングルコンテンツ

用であることを示す。鍵の有効期限は鍵データに示す鍵（コンテンツ鍵 $K_c$ 、および個別鍵 $K_i$ ）の使用期間をその期限の切れる日付、又は鍵の使用を開始した基準となる日から期限の切れる日までの日数などによって示し、コンテンツのIDはコンテンツ鍵 $K_c$ により暗号化するシングルコンテンツを示す。コンテンツプロバイダのIDはコンテンツを保有し、かつコンテンツ鍵 $K_c$ を生成したコンテンツプロバイダ2のIDを示す。

鍵のバージョンは使用期間に応じて改訂された鍵（コンテンツ鍵 $K_c$ 、および個別鍵 $K_i$ ）の改訂情報を示す。コンテンツ鍵 $K_c$ の暗号方式は個別鍵 $K_i$ を用いてコンテンツ鍵 $K_c$ を暗号化する際の暗号方式（例えば、DES）を示し、暗号化されたコンテンツ鍵 $K_c$ はその暗号方式により個別鍵 $K_i$ を用いて暗号化されたコンテンツ鍵 $K_c$ を示す。個別鍵 $K_i$ の暗号化方式は配送鍵 $K_d$ を用いて個別鍵 $K_i$ を暗号化する際の暗号方式（例えば、Triple-DES-CBC）を示し、暗号化された個別鍵 $K_i$ はその暗号方式により配送鍵 $K_d$ を用いて暗号化された個別鍵 $K_i$ を示す。署名はシングルコンテンツ用の鍵データから当該署名を除く、データの種別から公開鍵証明書までの全体に対して付けられるものである。署名を作成する際に用いたアルゴリズムおよびパラメータと、当該署名の検証に用いる鍵は公開鍵証明書に含まれている。

ここで、配送鍵 $K_d$ および個別鍵 $K_i$ はコンテンツプロバイダ2からシングルコンテンツ用の鍵データにより常に一体にされて配送される。そして、シングルコンテンツ用の鍵データにおいては、その全体に対して1つの署名が付加されている。従って、シングルコンテンツ用の鍵データを受け取った機器においては、暗号化されたコンテンツ鍵 $K_c$ および暗号化された個別鍵 $K_i$ に対してそれぞれ別々に署名を検証する必要がなく、シングルコンテンツ用の鍵データの1つの署名を検証するだけで当該暗号化されたコンテンツ鍵 $K_c$ および暗号化された個別鍵 $K_i$ に対する署名の検証をしたことになり、かくして、これら暗号化されたコンテンツ鍵 $K_c$ および暗号化された個別鍵 $K_i$ に対する署名の検証を簡易化し得る。



因みに、個別鍵 $K_i$ は、当該個別鍵 $K_i$ を用いてコンテンツ鍵 $K_c$ を暗号化するコンテンツプロバイダのIDと共に暗号化される。実際に、トリプルデスのCBCモードと呼ばれる暗号化方式によってコンテンツプロバイダのIDと共に個別鍵 $K_i$ を暗号化する方法を図49を用いて説明する。すなわち、かかる暗号化方式では、所定の初期値と、個別鍵 $K_i$  (64 bit) とを接続した後、配送鍵 $K_d$ を用いてトリプルデスのCBCモードによる暗号化方式で暗号化し、この結果、得られた64 bitの第1の値をコンテンツプロバイダのID (64 bit) と接続した後、再び配送鍵 $K_d$ を用いてトリプルデスのCBCモードによる暗号化方式で暗号化し、かくして、64 bitの第2の値を得る。そして、かかる暗号化方式では、第1の値と第2の値とを接続した16バイトのデータが、シングルコンテンツ用の鍵データに格納される暗号化された個別鍵 $K_i$ となる(この場合、第1の値はシングルコンテンツ用の鍵データに格納される暗号化された個別鍵 $K_i$ の始めの64 bitのデータに相当し、また、第2の値は当該シングルコンテンツ用の鍵データに格納される暗号化された個別鍵 $K_i$ 内の第1の値に続く64 bitのデータとなる)。

また、図50はアルバムコンテンツ用の鍵データを示すものであり、当該アルバムコンテンツ用の鍵データには、データの種別、鍵データの種類、鍵の有効期限、アルバムのID、コンテンツプロバイダのID、鍵のバージョン、アルバムを構成するシングルコンテンツの暗号化の際に用いるシングルコンテンツ用の鍵データの数、その鍵データの格納位置を示すアドレス情報、当該アドレス情報の示す位置に格納された鍵データパケット、公開鍵証明書、署名が格納されている。

アルバムコンテンツ用の鍵データにおいて、データの種別はこのデータが鍵のデータであることを示し、鍵データの種類は当該鍵データがアルバムコンテンツ用であることを示す。鍵の有効期限は鍵データに示す鍵(コンテンツ鍵 $K_c$ )の使用期間をその期限の切れる日付、又は鍵の使用を開始した基準となる日から期限の切れる日までの日数などによって示し、アルバムのIDはコンテンツ鍵 $K_c$ 。

により暗号化するシングルコンテンツからなるアルバムコンテンツを示す。コンテンツプロバイダのIDはアルバムコンテンツを暗号化するコンテンツプロバイダ2のIDを示す。

鍵のバージョンは使用期間に応じて改訂された鍵（コンテンツ鍵 $K_{co}$ ）の改訂情報を示す。署名はシングルコンテンツ用の鍵データから当該署名を除く、データの種別から公開鍵証明書までの全体に対して付けられるものである。署名を作成する際に用いたアルゴリズムおよびパラメータと、当該署名の検証に用いる鍵は公開鍵証明書に含まれている。

そして、アルバムコンテンツ用の鍵データにおいては、全体に対して署名を付けたことにより、当該署名を検証するだけで、当該アルバムコンテンツ用の鍵データに格納した複数のシングルコンテンツ用の鍵データの署名をそれぞれ検証しなくても当該アルバムコンテンツ用の鍵データと共に、各シングルコンテンツ用の鍵データに対しても合わせて改竄のチェックなどを行うことができ、かくして署名の検証を簡易化し得る。

図51は、1つの共通鍵で、共通鍵暗号であるDESを用いる、暗号処理部65と伸張部66との相互認証の動作を説明する図である。図51において、Aを伸張部66、Bを暗号処理部65とすると、暗号処理部65は64ビットの乱数 $R_B$ を生成し、 $R_B$ および自己のIDである $ID_B$ を、上位コントローラ62を介して伸張部66に送信する。これを受信した伸張部66は、新たに64ビットの乱数 $R_A$ を生成し、 $R_A$ 、 $R_B$ 、 $ID_B$ をDESのCBCモードで鍵 $K_{AB}$ を用いて暗号化し、上位コントローラ62を介して暗号処理部65に返送する。

DESのCBCモードとは、暗号化する際に、一つ前の出力と入力を排他的論理和し、それから暗号化する手法である。本例で言うならば、

$$X = \text{DES}(K_{AB}, R_A + IV) \quad IV = \text{初期値}, + : \text{排他的論理和}$$

$$Y = \text{DES}(K_{AB}, R_B + X)$$

$$Z = \text{DES}(K_{AB}, ID_B + Y)$$

となり、出力は、X、Y、Zとなる。これらの式において、 $\text{DES}(K_{AB}, R_A +$

IV) は鍵 $K_{AB}$ を使ってデータ $R_A + IV$ をDESで暗号化することを表し、 $DES(K_{AB}, R_B + X)$  は鍵 $K_{AB}$ を使ってデータ $R_B + X$ をDESで暗号化することを表し、 $DES(K_{AB}, ID_B + Y)$  は鍵 $K_{AB}$ を使ってデータ $ID_B + Y$ をDESで暗号化することを表す。

これを受信した暗号処理部65は、受信データを鍵 $K_{AB}$ で復号化し、 $R_B$  および  $ID_B$  が、暗号処理部65が送信したものと一致するか検査する。この検査に通った場合、伸張部66を正当なものとして認証する。続けて、セッション鍵（一時鍵 $K_{temp}$ のこと、乱数により生成する） $SK_{AB}$ を生成し、 $R_B$ 、 $R_A$ 、 $SK_{AB}$ をDESのCBCモードで鍵 $K_{AB}$ を用いて暗号化し、上位コントローラ62を介して伸張部66に送信する。これを受信した伸張部66は、受信データを鍵 $K_{AB}$ で復号化し、 $R_B$  および  $R_A$  が、伸張部66が送信したものと一致するか検査する。この検査に通った場合、暗号処理部65を正当なものとして認証し、データ $SK_{AB}$ をセッション鍵として以降の通信に使用する。なお、受信データの検査の際に、不正、不一致が見つかった場合には、相互認証が失敗したものとして処理を中断する。

図52は、公開鍵暗号である、160ビット長の楕円曲線暗号を用いる、ホームサーバ51の暗号処理部65内の相互認証モジュール95と据置機器52の暗号処理部73内の図示せぬ相互認証モジュールとの相互認証の動作を説明する図である。図52において、Aを暗号処理部73、Bを暗号処理部65とすると、暗号処理部65は、64ビットの乱数 $R_B$ を生成し、上位コントローラ62、通信部61を介して据置機器52へ送信する。これを受信した据置機器52は、暗号処理部73において新たに64ビットの乱数 $R_A$ 、および標数 $p$ より小さい乱数 $A_K$ を生成する。そして、ベースポイント $G$ を $A_K$ 倍した点 $A_V$ を求め、 $R_A$ 、 $R_B$ 、 $A_V$ （X座標とY座標）を接続し（64ビット+64ビット+160ビット+160ビットで、448ビットになる）、そのデータに対し、自己の持つ秘密鍵で署名データ $A.Sig$ を生成する。なお、ベースポイントのスカラー倍は図10の署名の生成で説明した方法と同じであるためその説明は省略する。データ

の接続とは、例えば次のようになる。16ビットのデータAと16ビットのデータBを接続すると、上位16ビットのデータがAで、下位16ビットのデータがBになる32ビットのデータのことを言う。署名の生成は図10の署名の生成で説明した方法と同じであるためその説明は省略する。

次に、暗号処理部73は、 $R_A$ 、 $R_B$ 、 $A_V$  および署名データA、 $Sig$ を上位コントローラ72に引き渡し、上位コントローラ72は、据置機器52用の公開鍵証明書（小容量記憶部75に保存されている）を追加して通信部71を介してホームサーバ51に送信する。公開鍵証明書は図32で説明しているのでその詳細は省略する。これを受信したホームサーバ51は、暗号処理部65において据置機器52の公開鍵証明書の署名を検証する。署名の検証は、図11の署名の検証で説明した方法と同じであるためその説明は省略する。次に、送られてきたデータのうち、乱数 $R_B$ が、暗号処理部65が送信したものと同一かどうか検査し、同一であった場合には署名データA、 $Sig$ を検証する。検証に成功したとき、暗号処理部65は暗号処理部73を認証する。なお、署名の検証は図11の署名の検証で説明した方法と同じであるためその説明は省略する。そして、暗号処理部65は、標数 $p$ より小さい乱数 $B_X$ を生成し、ベースポイント $G$ を $B_X$ 倍した点 $B_V$ を求め、 $R_B$ 、 $R_A$ 、 $B_V$ （X座標とY座標）を接続し、そのデータに対し、自己の持つ秘密鍵で署名データB、 $Sig$ を生成する。最後に、暗号処理部65は、 $R_B$ 、 $R_A$ 、 $B_V$  および署名データB、 $Sig$ を上位コントローラ62に引き渡し、上位コントローラ62は、ホームサーバ51用の公開鍵証明書（大容量記憶部68に保存されている）を追加して通信部61を介して据置機器52に送信する。

これを受信した据置機器52は、暗号処理部73においてホームサーバ51の公開鍵証明書の署名を検証する。次に、送られてきたデータのうち、乱数 $R_A$ が、暗号処理部73が送信したものと同一かどうか検査し、同一であった場合には署名データB、 $Sig$ を検証する。検証に成功したとき、暗号処理部73は暗号処理部65を認証する。

両者が認証に成功した場合には、暗号処理部 65 は  $B_K A_V$  ( $B_K$  は乱数だが、 $A_V$  は楕円曲線上の点であるため、楕円曲線上の点のスカラー倍計算が必要) を計算し、暗号処理部 73 は  $A_K B_V$  を計算し、これら点の X 座標の下位 64 ビットをセッション鍵 (一時鍵  $K_{temp}$ ) として以降の通信に使用する (共通鍵暗号を 64 ビット鍵長の共通鍵暗号とした場合)。因に、通信に使用するセッション鍵としては、X 座標の下位 64 ビットに限らず、Y 座標の下位 64 ビットを用いるようにしても良い。なお、相互認証後の秘密通信においては、データは一時鍵  $K_{temp}$  で暗号化されるだけでなく、その暗号化された送信データに署名が付されることがある。

署名の検証、受信データの検証の際に、不正、不一致が見つかった場合には、相互認証が失敗したものととして処理を中断する。

図 53 は、ユーザホームネットワーク 5 内の決済可能機器が、電子配信サービスセンタ 1 へ課金情報を送信するときの動作を説明する図である。ユーザホームネットワーク 5 内の決済可能機器は、登録情報から代理決済すべき対象機器を検索し、相互認証を行い、課金情報を共有した一時鍵  $K_{temp}$  (この鍵は、相互認証するたびに異なる) で暗号化して送らせる (このとき、データに署名が付いている)。全ての機器について処理が終わった後、電子配信サービスセンタ 1 と相互認証をし、共有した一時鍵で全ての課金情報を暗号化し、これらに署名データを付け、登録情報、必要に応じて取扱方針、価格情報と共に電子配信サービスセンタ 1 に送信する。なお、ユーザホームネットワーク 5 から電子配信サービスセンタ 1 へ送信される課金情報に、取扱方針の ID や価格情報の ID 等の金額の分配に必要な情報が含まれていることにより、情報量の多い取扱方針や価格情報は必ずしも送信する必要はない。ユーザ管理部 18 はこれを受信する。ユーザ管理部 18 は、受信した課金情報、登録情報、取扱方針、および価格情報に対する署名データの検証を行う。署名の検証は図 11 で説明した方法と同じなため詳細は省略する。次に、ユーザ管理部 18 は、相互認証のときに共有した一時鍵  $K_{temp}$  で課金情報を復号化し、取扱方針、および価格情報と共に経歴データ管理部 15 に送信す

る。

因みに、この実施の形態においては、相互認証後に送信されるデータは必要に応じて一時鍵 $K_{temp}$ で暗号化される。例えばコンテンツ鍵 $K_c$ や配送鍵 $K_d$ は内容が見られてしまうとデータを不正に利用されてしまうため一時鍵 $K_{temp}$ で暗号化して外部から見えないようにする必要がある。これに対して課金情報や使用許諾条件情報等は内容が見られても、データを不正に利用することができないため、必ずしも一時鍵 $K_{temp}$ で暗号化する必要はないが、例えば課金情報の金額が改竄されたり使用許諾条件情報の使用条件が緩くなるように改竄されると金額の授受に関係する当事者に損害が発生することになる。従って、課金情報や使用許諾条件情報には署名を付して送信することにより改竄を防止している。ただし、コンテンツ鍵 $K_c$ や配送鍵 $K_d$ を送信する場合にも署名を付けても良い。

そして、送信側では送られるデータに対して、又は送られるデータを一時鍵 $K_{temp}$ で暗号化したデータに対して署名を生成し、データ及び署名を送信する。受信側では、送られたデータが一時鍵 $K_{temp}$ で暗号化されていない場合には署名を検証することによりデータを得、又は送られたデータが一時鍵 $K_{temp}$ で暗号化されている場合には署名を検証した後に一時鍵 $K_{temp}$ でデータを復号することによりデータを得る。この実施の形態において、相互認証後に送信されるデータについては、以上の方法により署名及び必要に応じて一時鍵 $K_{temp}$ による暗号化が施される場合がある。

ユーザ管理部 18 は、鍵サーバ 14 から配送鍵 $K_d$ を受信し、これを共有した一時鍵 $K_{temp}$ で暗号化して署名データを付加し、ユーザ登録データベースから登録情報を作成し、一時鍵 $K_{temp}$ で暗号化された配送鍵 $K_d$ 、署名データ、登録情報をユーザホームネットワーク 5 内の決済可能機器に送信する。登録情報の作成方法については、図 8 で説明した通りでありここでの詳細説明は省略する。

課金請求部 19 は、決済を実行するとき、経歴データ管理部 15 から課金情報、必要に応じて取扱方針、および価格情報を受信し、ユーザへの請求金額を算出し、請求情報を出納部 20 に送信する。出納部 20 は、銀行等と通信し、決済処

理を実行する。その際、ユーザの未払い料金等の情報があれば、それらの情報は決済報告の形で課金請求部 19 およびユーザ管理部 18 に送信され、ユーザ登録データベースに反映され、以降のユーザ登録処理、または決済処理時に参照される。

一時鍵  $K_{temp}$  で暗号化された配送鍵  $K_d$ 、署名データ、登録情報を受信したユーザホームネットワーク 5 内の決済可能機器は、記憶してあった登録情報を更新すると共に、登録情報を検査し、登録がなされていれば、署名データを検証した後、配送鍵  $K_d$  を一時鍵  $K_{temp}$  で復号化し、暗号処理部内の記憶モジュールに記憶されている配送鍵  $K_d$  を更新し、記憶モジュール内の課金情報を削除する。続いて、登録情報から代理決済すべき対象機器を検索し、当該検索により見つかった機器ごとに相互認証を行い、暗号処理部の記憶モジュールから読み出した配送鍵  $K_d$  を検索により見つかった機器ごとに異なる一時鍵  $K_{temp}$  で暗号化し、それぞれの機器ごとに署名を付け登録情報と共にそれぞれの機器に送信する。代理決済すべき対象機器が全て終わった時点で処理が終了する。

これらのデータを受信した対象機器は、決済可能機器と同様に登録情報を検査し、署名データを検証した後、配送鍵  $K_d$  を一時鍵  $K_{temp}$  で復号化し、記憶モジュール内の配送鍵  $K_d$  を更新し、課金情報を削除する。

なお、登録情報の登録項目が「登録不可」となっていた機器については、課金が行われなかったため、配送鍵  $K_d$  の更新、課金情報の削除は行わない（登録項目の内容は、使用を含めて一切の停止、購入処理の停止、処理が正常に行われた状態等、記述されていない種々の場合があり得る）。

図 54 は電子配信サービスセンタ 1 の利益分配処理の動作を説明する図である。経歴データ管理部 15 は、ユーザ管理部 18 から送信された課金情報、必要に応じて取扱方針、および価格情報を保持・管理する。利益分配部 16 は、経歴データ管理部 15 から送信された課金情報、必要に応じて取扱方針および価格情報からコンテンツプロバイダ 2、サービスプロバイダ 3、および電子配信サービスセンタ 1 それぞれの利益を算出し、その結果をサービスプロバイダ管理部 11、

コンテンツプロバイダ管理部 12、および出納部 20 に送信する。出納部 20 は、銀行等と通信し、決済を行う。サービスプロバイダ管理部 11 は、利益分配部 16 から受信した分配情報をサービスプロバイダ 2 に送信する。コンテンツプロバイダ管理部 12 は、利益分配部 16 から受信した分配情報をコンテンツプロバイダ 3 に送信する。

監査部 21 は、経歴データ管理部 15 から課金情報、取扱方針、および価格情報を受信し、データに矛盾がないか監査する。例えば、課金情報内の価格が価格情報のデータと一致しているかどうか、分配率が一致しているかどうか等を監査し、取扱方針と価格情報が矛盾していないかどうか監査する。また、監査部 21 の処理としては、ユーザホームネットワーク 5 から入金された金額と、利益分配した合計金額又はサービスプロバイダ 3 へ送った金額との整合性を監査する処理や、ユーザホームネットワーク 5 の機器から供給された課金情報内のデータに例えば存在し得ないコンテンツプロバイダ ID、サービスプロバイダ ID や考えられない取り分、価格等が含まれているか否かを監査する処理がある。

図 55 は、電子配信サービスセンタ 1 の、コンテンツの利用実績を JASRAC に送信する処理の動作を説明する図である。経歴データ管理部 15 は、ユーザのコンテンツの利用実績を示す課金情報を著作権管理部 13 および利益分配部 16 に送信する。利益分配部 16 は、課金情報から JASRAC に対する請求金額および支払金額を算出し、支払情報を出納部 20 に送信する。出納部 20 は、銀行等と通信し、決済処理を実行する。著作権管理部 13 は、ユーザのコンテンツの利用実績を JASRAC に送信する。

次に、EMD システムの処理について説明する。図 56 は、このシステムのコンテンツの配布および再生の処理を説明するフローチャートである。ステップ S40 において、電子配信サービスセンタ 1 のコンテンツプロバイダ管理部 12 は、コンテンツプロバイダ 2 に個別鍵  $K_i$ 、配送鍵  $K_d$  で暗号化された個別鍵  $K_i$  およびコンテンツプロバイダ 2 の公開鍵証明書を送信し、コンテンツプロバイダ 2 がこれを受信する。その処理の詳細は、図 57 のフローチャートを参照して後述



する。ステップS 4 1において、ユーザは、ユーザホームネットワーク5の機器（例えば、図15のホームサーバ51）を操作し、ユーザホームネットワーク5の機器を電子配信サービスセンタ1のユーザ管理部18に登録する。この登録処理の詳細は、図59のフローチャートを参照して後述する。ステップS 4 2において、電子配信サービスセンタ1のユーザ管理部18は、ユーザホームネットワーク5と、図52について上述したように相互認証した後、ユーザホームネットワーク5の機器に、配送鍵 $K_d$ を送信する。ユーザホームネットワーク5はこの鍵を受信する。この処理の詳細は、図62のフローチャートを参照して説明する。

ステップS 4 3において、コンテンツプロバイダ2の署名生成部38は、コンテンツプロバイダセキュアコンテナを生成し、それをサービスプロバイダ3に送信する。この処理の詳細は、図65のフローチャートを参照して後述する。ステップS 4 4において、サービスプロバイダ3の署名生成部45は、サービスプロバイダセキュアコンテナを生成し、それをユーザホームネットワーク5へ、ネットワーク4を介して送信する。この送信処理の詳細は、図66のフローチャートを参照して後述する。ステップS 4 5において、ユーザホームネットワーク5の購入モジュール94は、購入処理を実行する。購入処理の詳細は、図67のフローチャートを参照して後述する。ステップS 4 6において、ユーザは、ユーザホームネットワーク5の機器でコンテンツを再生する。再生処理の詳細は、図72のフローチャートを参照して後述する。

図57は、図56のS 4 0に対応する、電子配信サービスセンタ1がコンテンツプロバイダ2へ個別鍵 $K_i$ 、配送鍵 $K_d$ で暗号化された個別鍵 $K_i$ および公開鍵証明書を送信し、コンテンツプロバイダ2がこれを受信する処理の詳細を説明するフローチャートである。ステップS 5 0において、電子配信サービスセンタ1の相互認証部17は、コンテンツプロバイダ2の相互認証部39と相互認証する。この相互認証処理は、図52で説明したので、その詳細は省略する。相互認証処理により、コンテンツプロバイダ2が正当なプロバイダであることが確認され

たとき、ステップS 5 1において、コンテンツプロバイダ2は、電子配信サービスセンタ1のコンテンツプロバイダ管理部1 2から送信された個別鍵 $K_1$ 、配送鍵 $K_d$ で暗号化された個別鍵 $K_1$ および証明書を受信する。ステップS 5 2において、コンテンツプロバイダ2は受信した個別鍵 $K_1$ を耐タンパメモリ4 0 Aに保存し、配送鍵 $K_d$ で暗号化された個別鍵 $K_1$ および証明書をメモリ4 0 Bに保存する。

このように、コンテンツプロバイダ2は、電子配信サービスセンタ1から個別鍵 $K_1$ 、配送鍵 $K_d$ で暗号化された個別鍵 $K_1$ および証明書を受け取る。同様に、図5 6に示すフローチャートの処理を行う例の場合、コンテンツプロバイダ2以外に、サービスプロバイダ3も、図5 7と同様の処理で、電子配信サービスセンタ1から個別鍵 $K_1$ （コンテンツプロバイダ2の個別鍵 $K_1$ とは異なる）、配送鍵 $K_d$ で暗号化された個別鍵 $K_1$ および証明書を受け取る。

なお、メモリ4 0 Aは、コンテンツプロバイダ2が秘密裏に保持しなくてはならない個別鍵 $K_1$ を保持するため、第3者に容易にデータを読み出されない耐タンパメモリが望ましいが、特にハードウェア的制限は必要ない（例えば、入室管理された部屋の中にあるハードディスクや、パスワード管理されたパソコンのハードディスク等でよい）。また、メモリ4 0 Bは、配送鍵 $K_d$ で暗号化された個別鍵 $K_1$ 、コンテンツプロバイダ2の証明書が保存されるだけであるため、通常の記憶装置等何でもよい（秘密にする必要がない）。また、メモリ4 0 A、4 0 Bを一つにしてもかまわない。

図5 8は、ホームサーバ5 1が、電子配信サービスセンタ1のユーザ管理部1 8に決済情報を登録する処理を説明するフローチャートである。ステップS 6 0において、ホームサーバ5 1は、大容量記憶部6 8に記憶されている公開鍵証明書を、暗号処理部6 5の相互認証モジュール9 5で、電子配信サービスセンタ1の相互認証部1 7と相互認証する。この認証処理は、図5 2を参照して説明した場合と同様であるので、ここでは説明を省略する。ステップS 6 0で、ホームサーバ5 1が電子配信サービスセンタ1のユーザ管理部1 8に送信する証明書は、

図 3 2 に示すデータ（ユーザ機器の公開鍵証明書）を含む。

ステップ S 6 1 において、ホームサーバは個人の決済情報（ユーザのクレジットカード番号や、決済機関の口座番号等）の登録が新規登録か否かを判定し、新規登録であると判定された場合、ステップ S 6 2 に進む。ステップ S 6 2 において、ユーザは入力手段 6 3 を用いて個人の決済情報を入力する。これらのデータは、暗号化ユニット 1 1 2 で一時鍵  $K_{temp}$  を用いて暗号化され、通信部 6 1 を介して電子配信サービスセンタ 1 のユーザ管理部 1 8 に送信される。

ステップ S 6 3 において、電子配信サービスセンタ 1 のユーザ管理部 1 8 は、受信した証明書から機器の ID を取り出し、この機器の ID を基に、図 7 に示したユーザ登録データベースを検索する。ステップ S 6 4 において、電子配信サービスセンタ 1 のユーザ管理部 1 8 は、受信した ID を有する機器の登録が可能であるか否かを判定し、受信した ID を有する機器の登録が可能であると判定された場合、ステップ S 6 5 に進み、受信した ID を有する機器が、新規登録であるか否かを判定する。ステップ S 6 5 において、受信した ID を有する機器が、新規登録であると判定された場合には、ステップ S 6 6 に進む。

ステップ S 6 6 において、電子配信サービスセンタ 1 のユーザ管理部 1 8 は、決済 ID を新規に発行すると共に、一時鍵で暗号化された決済情報を復号化し、決済 ID および決済情報を、機器 ID、決済 ID、決済情報（口座番号やクレジットカード番号等）、取引停止情報等を記憶している決済情報データベースに機器の ID に対応させて登録し、決済 ID をユーザ登録データベースに登録する。ステップ 6 7 において、ユーザ登録データベースに登録したデータに基づき登録情報を作成する。この登録情報は、図 8 で説明しているので、その詳細は省略する。

ステップ S 6 8 において、電子配信サービスセンタ 1 のユーザ管理部 1 8 は、作成した登録情報をホームサーバ 5 1 に送信する。ステップ S 6 9 において、ホームサーバ 5 1 の上位コントローラ 6 2 は、受信した登録情報を大容量記憶部 6 8 に保存する。

ステップS 6 1において、決済情報の登録が更新登録であると判定された場合、手続きは、ステップS 7 0に進み、ユーザは入力手段6 3を用いて個人の決済情報を入力する。これらのデータは、暗号化ユニット1 1 2で一時鍵 $K_{temp}$ を用いて暗号化され、既に決済登録時に発行された登録情報と共に通信部6 1を介して電子配信サービスセンタ1のユーザ管理部1 8に送信される。

ステップS 6 4において、受信したIDを有する機器の登録が不可であると判定された場合、ステップS 7 1に進み、電子配信サービスセンタ1のユーザ管理部1 8は、登録拒絶の登録情報を作成し、ステップS 6 8に進む。

ステップS 6 5において、受信したIDを有する機器が、新規登録でないと判定された場合、手続きは、ステップS 7 2に進み、電子配信サービスセンタ1のユーザ管理部1 8は、一時鍵で暗号化された決済情報を復号化し、機器のIDに対応させて決済情報登録データベースに更新登録し、ステップS 6 7に進む。

このように、ホームサーバ5 1は、電子配信サービスセンタ1に登録される。

図5 9は、登録情報に機器のIDを新規登録する処理を説明するフローチャートである。ステップS 8 0における相互認証処理は、図5 2で説明した処理と同様なため、説明を省略する。ステップS 8 1において、図5 8のステップS 6 3と同じであるためその説明は省略する。ステップS 8 2は、図5 8のステップS 6 4と同じであるためその説明は省略する。ステップS 8 3において、電子配信サービスセンタ1のユーザ管理部1 8は、ユーザ登録データベース内の機器IDに対応する登録項目を「登録」に設定し、機器IDを登録する。ステップS 8 4において、電子配信サービスセンタ1のユーザ管理部1 8は、ユーザ登録データベースに基づき、図8に示すような登録情報を作成する。ステップS 8 5は、図5 8のステップS 6 8と同じであるためその説明は省略する。ステップS 8 6は、図5 8のステップS 6 9と同じであるためその説明は省略する。

ステップS 8 2において、受信したIDを有する機器の登録が不可であると判定された場合、ステップS 8 7に進み、電子配信サービスセンタ1のユーザ管理部1 8は、登録拒絶の登録情報を作成し、ステップS 8 5に進む。

このように、ホームサーバ51は、電子配信サービスセンタ1に登録される。

図60は、既に登録された機器を経由し、別の機器を追加登録する際の処理を説明するフローチャートである。ここでは、ホームサーバ51が既に登録されており、そこに据置機器52を登録する例で説明する。ステップS90において、ホームサーバ51は、据置機器52と相互認証する。相互認証処理は、図52で説明した処理と同様なため、説明を省略する。ステップS91において、ホームサーバ51は、電子配信サービスセンタ1と相互認証する。ステップS92において、ホームサーバ51は、大容量記憶部68から読み出した登録情報、およびステップS90で据置機器52と相互認証した際に入手した据置機器52の証明書を電子配信サービスセンタ1に送信する。ステップS93は、図59のステップS81と同じであるためその説明は省略する。ステップS94は、図59のステップS82と同じであるためその説明は省略する。ステップS95は、図59のステップS83と同じであるためその説明は省略する。ステップS96において、電子配信サービスセンタ1のユーザ管理部18は、ホームサーバ51から受信した登録情報に加え、据置機器52の情報を追加した登録情報を新規に作成する。ステップS97は、図59のステップS85と同じであるためその説明は省略する。ステップS98は、図59のステップS86と同じであるためその説明は省略する。

そして、ステップS99Aにおいてホームサーバ51は受信した登録情報を据置機器52に送信し、ステップS99Bにおいて据置機器52は受信した登録情報を小容量記憶部75に保存する。

ステップS94において、受信したIDを有する機器の登録が不可であると判定された場合、ステップS99に進み、電子配信サービスセンタ1のユーザ管理部18は、据置機器52のみ登録拒絶とした登録情報（従って、ホームサーバ51は登録済みのまま）を作成し、ステップS97に進む（ステップS91でホームサーバ51が電子配信サービスセンタ1と相互認証に成功しているということは、ホームサーバ51が登録可であることを意味している）。

かくして、据置機器 5 2 は、図 6 0 に示した処理手順により電子配信サービスセンタ 1 に追加登録される。

ここで、登録済の機器が登録の更新（登録情報の更新）を行うタイミングについて説明する。図 6 1 は登録情報の更新を行うか否かを種々の条件に基づいて判断する処理手順を示し、ステップ S 6 0 0 においてホームサーバ 5 1 は配送鍵 K<sub>d</sub>、登録情報又は課金情報のすい上げから予め決められた一定期間が経過したか否かを時計（図示せず）及び判断部（図示せず）によって判断する。ここで肯定結果が得られると、このことは配送鍵 K<sub>d</sub>、登録情報又は課金情報のすい上げから一定の期間が経過していることを表しており、このときホームサーバ 5 1 はステップ S 6 0 7 に移って登録情報の更新処理を実行する。この処理については図 6 2 において後述する。

これに対してステップ S 6 0 0 において否定結果が得られると、このことは配送鍵 K<sub>d</sub>、登録情報又は課金情報のすい上げから一定の期間が経過していないこと、すなわち期間の経過について登録情報の更新条件を満たしていないことを表しており、このときホームサーバ 5 1 はステップ S 6 0 1 に移る。

ステップ S 6 0 1 においてホームサーバ 5 1 は、コンテンツの購入回数が規定の回数に達しているか否かを判断する。ここで肯定結果が得られると、ホームサーバ 5 1 はステップ S 6 0 7 に移って登録情報更新処理を実行し、これに対してステップ S 6 0 1 において否定結果が得られると、このことはコンテンツの購入回数について登録情報の更新条件を満たしていないことを表していることによりホームサーバ 5 1 は続くステップ S 6 0 2 に移る。

ステップ S 6 0 2 において、ホームサーバ 5 1 は、コンテンツの購入金額が規定の金額に達しているか否かを判断する。ここで肯定結果が得られると、ホームサーバ 5 1 はステップ S 6 0 7 に移って登録情報更新処理を実行し、これに対してステップ S 6 0 2 において否定結果が得られると、このことはコンテンツの購入金額について登録情報の更新条件を満たしていないことを表していることによりホームサーバ 5 1 は続くステップ S 6 0 3 に移る。

ステップS 6 0 3において、ホームサーバ5 1は、配送鍵K<sub>d</sub>の有効期限が切れているか否かを判断する。配送鍵K<sub>d</sub>の有効期限が切れているか否かを判断する方法としては、配信されたデータの配送鍵K<sub>d</sub>のバージョンが記憶モジュール9 2に保存されている3つのバージョンの配送鍵K<sub>d</sub>のいずれかのバージョンと一致するか否か又は、最近の配送鍵K<sub>d</sub>のバージョンより古いかなどを調べる。この比較結果が一致していない場合又は最近の配送鍵K<sub>d</sub>のバージョンより古い場合には、記憶モジュール9 2内の配送鍵K<sub>d</sub>の有効期限が切れていることになり、ホームサーバ5 1はステップS 6 0 3において肯定結果を得ることによりステップS 6 0 7に移って登録情報の更新処理を実行する。これに対してステップS 6 0 3において否定結果が得られると、このことは配送鍵K<sub>d</sub>の有効期限について登録情報の更新条件を満たしていないことを表しており、このときホームサーバ5 1は続くステップS 6 0 4に移る。

ステップS 6 0 4において、ホームサーバ5 1は、当該ホームサーバ5 1に他機器が新規接続されたか否か、又は接続されていた他機器が切り離されたか否かといったネットワーク構成の変更の有無を判断する。ここで肯定結果が得られると、このことはネットワーク構成に変更があったことを表しており、このときホームサーバ5 1はステップS 6 0 7に移って登録情報の更新処理を実行する。これに対してステップS 6 0 4において否定結果が得られると、このことはネットワーク構成について登録情報の更新条件を満たしていないことを表しており、ホームサーバ5 1は続くステップS 6 0 5に移る。

ステップS 6 0 5において、ホームサーバ5 1は、ユーザからの登録情報更新要求があったか否かを判断し、登録情報更新要求があった場合にはステップS 6 0 7に移って登録情報の更新処理を実行し、登録情報更新要求がなかった場合にはステップS 6 0 6に移る。

ステップS 6 0 6において、ホームサーバ5 1は接続された他の機器について上述のステップS 6 0 0～ステップS 6 0 5における更新判断を行い、更新すべき判断結果が得られたときステップS 6 0 7に移って登録情報の更新処理を行い

、これに対して更新すべき判断結果が得られないとき上述のステップS 6 0 0 から同様の処理を繰り返す。これにより、ホームサーバ5 1は登録情報の更新処理を行うタイミングを得ることができる。なお、ホームサーバ5 1が他の機器の更新開始条件を調べるのではなく、他の機器が独自に調べて、自らホームサーバ5 1に要求を出すようにしてもよい。

図6 2は、登録済みの機器が登録を更新（登録情報の更新）し、決済処理を行い、配送鍵 $K_d$ の再配布を受ける動作を説明するフローチャートである。ステップS 1 0 0における相互認証処理は、図5 2で説明した処理と同様なため、説明を省略する。ステップS 1 0 1において、ホームサーバ5 1は、記憶モジュール9 2に記憶されている課金情報を、暗号処理部9 6の暗号化ユニット1 1 2で一時鍵 $K_{temp}$ を用いて暗号化し、署名生成ユニット1 1 4で署名を生成し、署名を付加する。そして、暗号化された課金情報及びその署名と、大容量記憶部6 8に記憶されている取扱方針、価格情報および登録情報を合わせて電子配信サービスセンタ1に送信する。なお、このとき、取扱方針および価格情報はモデルによっては送信する必要がない。なぜなら、コンテンツプロバイダ2およびサービスプロバイダ3が予め電子配信サービスセンタ1に送信している場合があったり、課金情報に取扱方針、価格情報のうちの必要な情報が含まれている場合があるからである。

ステップS 1 0 2は、図5 9のステップS 8 1と同じであるためその説明は省略する。ステップS 1 0 3は、図5 9のステップS 8 2と同じであるためその説明は省略する。ステップS 1 0 4において、電子配信サービスセンタ1のユーザ管理部1 8は署名検証ユニット1 1 5で署名を検証し、受信した課金情報を一時鍵 $K_{temp}$ で復号化し（受信データに電子署名がついている場合には、署名検証ユニット1 1 5で検証する）、（受信していれば）取扱方針および価格情報と共に経歴データ管理部1 5に送信する。これを受信した経歴データ管理部1 5は、受信データを保存・管理する。

ステップS 1 0 5において、電子配信サービスセンタ1のユーザ管理部1 8は



、ユーザ登録データベース内の機器IDに対応する登録項目を検証すると共に、データを更新する。例えば、図示せぬ登録日付や課金状況などのデータである。ステップS106は、図59のステップS84と同じであるためその説明は省略する。ステップS107において、電子配信サービスセンタ1のユーザ管理部は、鍵サーバ14から供給された配送鍵 $K_d$ を一時鍵 $K_{temp}$ で暗号化し、登録情報と共にホームサーバ51に送信する。

ステップS108において、ホームサーバ51は受信した登録情報を大容量記憶部68に保存する。ステップS109において、ホームサーバ51は、受信した登録情報を暗号処理部65に入力し、暗号処理部65では、登録情報に含まれる電子署名を署名検証ユニット115で検証すると共に、ホームサーバ51の機器IDが登録されているか確認させ、検証に成功し、課金処理が完了したことを確認した際にはステップS110に進む。ステップS110において、ホームサーバ51は、受信した配送鍵 $K_d$ を暗号処理部65に入力する。暗号処理部65では、受信した配送鍵 $K_d$ を暗号／復号化モジュール96の復号化ユニット111で一時鍵 $K_{temp}$ を用いて復号化し、記憶モジュール92に保存（更新）し、記憶モジュール92に保持していた課金情報を消去する（これで、決済済みとなる）。

ステップS103において、受信したIDを有する機器の登録が不可であると判定された場合、ステップS111に進み、電子配信サービスセンタ1のユーザ管理部18は、登録拒絶とした登録情報を作成し、ステップS112に進む。ステップS112では、ステップS107と異なり、登録情報のみをホームサーバ51に送信する。

ステップS109において、登録情報に含まれる署名の検証に失敗するか、登録情報に含まれる「登録」の項目（例えば、課金処理失敗→購入処理ができない、登録拒否→再生等の処理を含め暗号処理部の機能の停止、取引一時停止→課金処理は成功したが、何らかの理由で購入を停止する、等が考えられる）に「登録可」が書かれていない場合は、ステップS113に進み所定のエラー処理を行う。

このように、ホームサーバ 5 1 は、登録情報を更新すると共に、課金情報を電子配信サービスセンタ 1 に送信し、代わりに配送鍵  $K_d$  の供給を受ける。

図 6 3 及び図 6 4 は、据置機器 5 2 がホームサーバ 5 1 を介して決済、登録情報の更新、配送鍵  $K_d$  の更新を行う処理を説明するフローチャートを示した図である。ステップ S 1 2 0 において、ホームサーバ 5 1 の相互認証モジュール 9 4 と据置機器の図示せぬ相互認証モジュールは、相互認証を行う。相互認証処理は、図 5 2 で説明した処理と同様なため、説明を省略する。なお、相互認証処理で説明したように、ホームサーバ 5 1 と据置機器 5 2 は互いに証明書を交換し合っているため、相手の機器 ID はわかっているものとする。ステップ S 1 2 1 において、ホームサーバ 5 1 の上位コントローラ 6 2 は、大容量記憶部 6 8 から登録情報を読み出し、暗号処理部 6 5 に検査させる。上位コントローラ 6 2 から登録情報を受け取った暗号処理部 6 5 は、登録情報内の署名を検証し、据置機器の ID があるかどうか判定し、登録情報に据置機器の ID があつた際にはステップ S 1 2 2 に進む。

ステップ S 1 2 2 において、登録情報に据置機器 5 2 の ID が登録されているか否かを判定し、据置機器 5 2 の ID が登録されている場合には、ステップ S 1 2 3 に進む。ステップ S 1 2 3 において、据置機器 5 2 の暗号処理部 7 3 は、記憶モジュールに保存されている課金情報を読み出し、暗号化ユニットで一時鍵  $K_{temp}$  を用いて暗号化する。また、課金情報に対応する署名を、署名生成ユニットで生成する。署名の生成は図 1 0 で説明したのでその詳細は省略する。一時鍵  $K_{temp}$  で暗号化された課金情報およびその署名を受け取った上位コントローラ 7 2 は、必要に応じて課金情報に対応する取扱方針および価格情報を小容量記憶部 7 5 から読み出し、一時鍵  $K_{temp}$  で暗号化された課金情報とその署名、必要に応じて課金情報に対応する取扱方針および価格情報をホームサーバ 5 1 に送信する。

これらのデータを受信したホームサーバ 5 1 は、受信していれば取扱方針および価格情報を大容量記憶部 6 8 に記憶すると共に、一時鍵  $K_{temp}$  で暗号化された課

金情報およびその署名を暗号処理部 6 5 に入力する。一時鍵  $K_{temp}$  で暗号化された課金情報およびその署名を受信した暗号処理部 6 5 は、暗号／復号化モジュール 9 6 の署名検証ユニット 1 1 5 で、一時鍵  $K_{temp}$  で暗号化された課金情報に対する署名を検証する。署名の検証は図 1 1 で説明した処理と同じであるため、その詳細は省略する。そして、暗号／復号化モジュール 9 6 の復号化ユニット 1 1 1 は、一時鍵  $K_{temp}$  で暗号化された課金情報を復号化する。

ステップ S 1 2 4 において、ホームサーバ 5 1 は、電子配信サービスセンタ 1 の相互認証部 1 7 と相互認証し一時鍵  $K_{temp2}$  を共有する。ステップ S 1 2 5 において、ホームサーバ 5 1 は、据置機器 5 2 から送られてきた課金情報を暗号／復号化モジュール 9 6 の暗号化ユニット 1 1 2 で一時鍵  $K_{temp2}$  を用いて暗号化する。このとき、ホームサーバ 5 1 の課金情報を合わせて暗号化しておいてもよい。また、一時鍵  $K_{temp2}$  で暗号化された課金情報に対応する署名を、暗号／復号化モジュール 9 6 の署名生成ユニット 1 1 4 で生成する。一時鍵  $K_{temp2}$  で暗号化された課金情報、およびその署名を受け取った上位コントローラ 6 2 は、必要に応じて課金情報に対応する取扱方針、価格情報、および登録情報を大容量記憶部 6 8 から読み出し、一時鍵  $K_{temp2}$  で暗号化された課金情報、その署名、必要に応じて課金情報に対応する取扱方針、価格情報および登録情報を電子配信サービスセンタ 1 のユーザ管理部 1 8 に送信する。

ステップ S 1 2 6 において、電子配信サービスセンタ 1 のユーザ管理部 1 8 は、ユーザ登録データベースを検索する。ステップ S 1 2 7 において、ホームサーバ 5 1 および据置機器 5 2 がユーザ登録データベース内の「登録」の項目に、登録可で登録されているか否か判定し、登録されていると判定されていた場合、ステップ S 1 2 8 に進む。ステップ S 1 2 8 において、電子配信サービスセンタ 1 のユーザ管理部 1 8 は、一時鍵  $K_{temp2}$  で暗号化された課金情報に対する署名を検証し、課金情報を一時鍵  $K_{temp2}$  で復号化する。そして、課金情報、受信していれば取扱方針および価格情報を経歴データ管理部 1 5 に送信する。課金情報、受信していれば取扱方針および価格情報を受信した経歴データ管理部 1 5 は、そのデ

ータを管理・保存する。

ステップS 1 2 9において、電子配信サービスセンタ 1 のユーザ管理部 1 8 は、ユーザ登録データベースを更新する（図示せぬ課金データ受信日時、登録情報発行日時、配送鍵交付日時等）。ステップS 1 3 0において、電子配信サービスセンタ 1 のユーザ管理部 1 8 は、登録情報を作成する（例えば図 8 の例）。ステップS 1 3 1において、電子配信サービスセンタ 1 のユーザ管理部 1 8 は、電子配信サービスセンタ 1 の鍵サーバ 1 4 から受信した配送鍵 $K_d$ を一時鍵 $K_{temp2}$ で暗号化し、一時鍵 $K_{temp2}$ で暗号化された配送鍵 $K_d$ に対する署名を生成する。そして、登録情報、一時鍵 $K_{temp2}$ で暗号化された配送鍵 $K_d$ および一時鍵 $K_{temp2}$ で暗号化された配送鍵 $K_d$ に対する署名をホームサーバ 5 1 に送信する。

ステップS 1 3 2において、ホームサーバ 5 1 は、登録情報、一時鍵 $K_{temp2}$ で暗号化された配送鍵 $K_d$ および一時鍵 $K_{temp2}$ で暗号化された配送鍵 $K_d$ に対する署名を受信する。ホームサーバ 5 1 の上位コントローラ 6 2 は、一時鍵 $K_{temp2}$ で暗号化された配送鍵 $K_d$ および一時鍵 $K_{temp2}$ で暗号化された配送鍵 $K_d$ に対する署名を暗号処理部 6 5 に入力する。暗号処理部 6 5 において、暗号／復号化モジュール 9 6 の署名検証ユニット 1 1 5 は、一時鍵 $K_{temp2}$ で暗号化された配送鍵 $K_d$ に対する署名を検証し、暗号／復号化モジュール 9 6 の復号化ユニット 1 1 1 は、一時鍵 $K_{temp2}$ を用いて配送鍵 $K_d$ を復号化し、暗号／復号化モジュール 9 6 の暗号化ユニット 1 1 2 は、復号化された配送鍵 $K_d$ を、据置機器 5 2 との間で共有した一時鍵 $K_{temp}$ を用いて再暗号化する。最後に、暗号／復号化モジュール 9 6 の署名生成ユニット 1 1 4 は、一時鍵 $K_{temp}$ を用いて暗号化された配送鍵 $K_d$ に対応する署名を生成し、一時鍵 $K_{temp}$ で暗号化された配送鍵 $K_d$ および一時鍵 $K_{temp}$ で暗号化された配送鍵 $K_d$ に対する署名を上位コントローラ 6 2 に返送する。一時鍵 $K_{temp}$ で暗号化された配送鍵 $K_d$ および一時鍵 $K_{temp}$ で暗号化された配送鍵 $K_d$ に対する署名を受信した上位コントローラ 6 2 は、電子配信サービスセンタ 1 から送られてきた登録情報と共に据置機器 5 2 に送信する。

ステップS 1 3 3において、据置機器 5 2 の上位コントローラ 7 2 は、受信し

た登録情報を小容量記憶部 75 に上書き保存する。ステップ S 134 において、据置機器 52 の暗号処理部 73 は、受信した登録情報の署名を検証し、据置機器 52 の ID の「登録」に対する項目が「登録可」になっているか否かを判定し、「登録可」になっていた場合には、ステップ S 135 に進む。ステップ S 135 において、据置機器 52 の上位コントローラは、一時鍵  $K_{temp}$  で暗号化された配送鍵  $K_d$  および一時鍵  $K_{temp}$  で暗号化された配送鍵  $K_d$  に対する署名を暗号処理部 73 に入力する。暗号処理部 73 は、一時鍵  $K_{temp}$  で暗号化された配送鍵  $K_d$  に対する署名を検証し、一時鍵  $K_{temp}$  を用いて配送鍵  $K_d$  を復号化し、暗号処理部 73 の記憶モジュール内の配送鍵  $K_d$  を更新すると共に、課金情報を消去する（なお、実際には消去せず、決済済みのマークを付けるだけの場合がある）。

ステップ S 121 において、据置機器 52 の ID が登録情報に含まれていなかった場合、ステップ S 136 に進み、図 60 で説明した登録情報追加処理を開始し、ステップ S 123 へと進む。

ステップ S 127 において、ユーザ登録データベース内の「登録」項目に対し、ホームサーバ 51 の ID または据置機器 52 の ID が「登録可」になっていなかった場合、ステップ S 137 に進む。ステップ S 137 は、ステップ S 130 の場合と同様なため、その詳細は省略する。ステップ S 138 は、ステップ S 131 において、電子配信サービスセンタ 1 のユーザ管理部 18 は、登録情報をホームサーバ 51 に送信する。ステップ S 139 において、ホームサーバ 51 は、登録情報を据置機器 52 に送信する。

ステップ S 122 において、登録情報における据置機器 52 の ID に対する「登録」項目が、「登録可」になっていなかった場合、ステップ S 134 において、登録情報における据置機器 52 の ID に対する「登録」項目が、「登録可」になっていなかった場合、処理は終了する。

なお、本方式による代理処理は、据置機器 52 のみの処理になっているが、ホームサーバ 51 につながる全ての機器やホームサーバ 51 自身の課金情報を全て集め、一括処理しても良い。そして、全ての機器の登録情報、配送鍵  $K_d$  の更新

を行う（本実施例において、受け取った登録情報、配送鍵 $K_d$ は、ホームサーバ51で全くチェックされていない。ホームサーバ51自身の処理も一括して行う場合には、当然チェックし、更新すべきである）。

次に、図56のステップS43に対応する、コンテンツプロバイダ2がサービスプロバイダ3にコンテンツプロバイダセキュアコンテナを送信する処理を、図65のフローチャートを用いて説明する。ステップS140において、コンテンツプロバイダ2の電子透かし付加部32は、コンテンツサーバ31から読み出したコンテンツに、コンテンツプロバイダ2を示す所定のデータ、例えばコンテンツプロバイダIDなどを電子透かしの形で挿入し、圧縮部33に供給する。ステップS141において、コンテンツプロバイダ2の圧縮部33は、電子透かしが挿入されたコンテンツをATRAC等の所定の方式で圧縮し、コンテンツ暗号部34に供給する。ステップS142において、コンテンツ鍵生成部35は、コンテンツ鍵 $K_c$ として用いる鍵を生成させ、コンテンツ暗号部34およびコンテンツ鍵暗号部36に供給する。ステップS143において、コンテンツプロバイダ2のコンテンツ暗号部34は、DESなどの所定の方式で、コンテンツ鍵 $K_c$ を使用して、電子透かしが挿入され、圧縮されたコンテンツを暗号化する。

ステップS144において、コンテンツ鍵暗号部36は、DESなどの所定の方法で、図56のステップS40の処理により、電子配信サービスセンタ1から供給されている個別鍵 $K_i$ でコンテンツ鍵 $K_c$ を暗号化する。ステップS145において、取扱方針生成部37は、コンテンツの取り扱い方針を規定し、図33又は図3.4に示すような取扱方針を生成する。ステップS146において、コンテンツプロバイダ2の署名生成部38は、暗号化されたコンテンツ、暗号化されたコンテンツ鍵 $K_c$ 、暗号化された個別鍵 $K_i$ および取扱方針生成部37から供給された取扱方針に対し署名を生成する。署名の生成は図10を参照して説明した場合と同様であるので、ここでは説明を省略する。ステップS147において、コンテンツプロバイダ2は、暗号化されたコンテンツおよびその署名、暗号化されたコンテンツ鍵 $K_c$ およびその署名、暗号化された個別鍵 $K_i$ およびその署名

、取扱方針およびその署名（以降、これら4つの署名付きデータをコンテンツプロバイダセキュアコンテナと呼ぶ）、予め認証局からもらっておいたコンテンツプロバイダ2の証明書を、図示せぬ送信部を用いてサービスプロバイダ3に送信する。

以上のように、コンテンツプロバイダ2は、サービスプロバイダ3に、コンテンツプロバイダセキュアコンテナを送信する。

次に、図56のステップS44に対応する、サービスプロバイダ3がホームサーバ51にサービスプロバイダセキュアコンテナを送信する処理を、図66のフローチャートを用いて説明する。なお、サービスプロバイダ3は、コンテンツプロバイダ2から送信されたデータをコンテンツサーバ41に予め保存しているものとして説明する。ステップS150において、サービスプロバイダ3の証明書検証部42は、コンテンツサーバ41からコンテンツプロバイダ2の証明書の署名を読み出し、証明書内の署名を検証する。署名の検証は図11を参照して説明した方法と同様なため、その詳細は省略する。証明書に改竄がなければ、コンテンツプロバイダ2の公開鍵 $K_{pcp}$ を取り出す。

ステップS151において、サービスプロバイダ3の署名検証部43は、コンテンツプロバイダ2の送信部から送信されたコンテンツプロバイダセキュアコンテナの署名をコンテンツプロバイダ2の公開鍵 $K_{pcp}$ で検証する（取扱方針の署名のみ検証する場合がある）。署名の検証に失敗し、改竄が発見された場合は、処理を終了する。なお、署名の検証は図11を参照して説明した方法と同様なため、その詳細は省略する。

コンテンツプロバイダセキュアコンテナに改竄がない場合、ステップS152において、サービスプロバイダ3の値付け部44は、取扱方針を基に、図37や図38で説明した価格情報を作成する。ステップS153において、サービスプロバイダ3の署名生成部45は、価格情報に対する署名を生成し、コンテンツプロバイダセキュアコンテナ、価格情報、および価格情報の署名を合わせサービスプロバイダセキュアコンテナを作成する。

ステップS 1 5 4において、サービスプロバイダ3の図示せぬ送信部は、ホームサーバ5 1の通信部6 1に、サービスプロバイダ3の証明書、コンテンツプロバイダ2の証明書およびサービスプロバイダセキュアコンテナを送信し、処理を終了する。

このように、サービスプロバイダ3は、ホームサーバ5 1にサービスプロバイダセキュアコンテナを送信する。

図5 6のステップS 4 5に対応する、適正なサービスプロバイダセキュアコンテナを受信した後の、ホームサーバ5 1の購入処理の詳細を、図6 7のフローチャートを用いて説明する。ステップS 1 6 1において、ホームサーバ5 1は図6 1及び図6 2について上述した登録情報更新処理を実行した後、ステップS 1 6 2において、ホームサーバ5 1の上位コントローラ6 2は、ホームサーバ5 1の大容量記憶部6 8から読み出した登録情報をホームサーバ5 1の暗号処理部6 5に入力する。登録情報を受信した暗号処理部6 5は、暗号／復号化モジュール9 6の署名検証ユニット1 1 5で登録情報の署名を検証した後、ホームサーバ5 1のIDに対する「購入処理」の項目が「購入可」になっているか判定すると共に登録の項目が「登録可」になっていることを検査し、「購入可」及び「登録可」であった場合にはステップS 1 6 3に進む。なお、署名検証、「登録可」、「購入可」の検査は登録情報検査モジュール9 3で行うようにしても良い。ステップS 1 6 3において、ホームサーバ5 1の上位コントローラ6 2は、ホームサーバ5 1の大容量記憶部6 8から読み出したコンテンツプロバイダ2の公開鍵証明書をホームサーバ5 1の暗号処理部6 5に入力する。

コンテンツプロバイダ2の公開鍵証明書を受信した暗号処理部6 5は、暗号／復号化モジュール9 6の署名検証ユニット1 1 5でコンテンツプロバイダ2の証明書の署名を検証した後、公開鍵証明書からコンテンツプロバイダ2の公開鍵を取り出す。署名の検証の結果、改竄がなされていないことが確認された場合には、ステップS 1 6 4に進む。ステップS 1 6 4において、ホームサーバ5 1の上位コントローラ6 2は、ホームサーバ5 1の大容量記憶部6 8から読み出したコ



コンテンツをホームサーバ51の暗号処理部65に入力する。コンテンツを受信した暗号処理部65は、暗号／復号化モジュール96の署名検証ユニット115でコンテンツの署名を検証し、改竄がなされていないことが確認された場合には、ステップS165に進む。ステップS165において、ホームサーバ51の上位コントローラ62は、ホームサーバ51の大容量記憶部68から読み出したコンテンツ鍵 $K_c$ をホームサーバ51の暗号処理部65に入力する。

コンテンツ鍵 $K_c$ を受信した暗号処理部65は、暗号／復号化モジュール96の署名検証ユニット115でコンテンツ鍵 $K_c$ の署名を検証し、改竄がなされていないことが確認された場合には、ステップS166に進む。ステップS166において、ホームサーバ51の上位コントローラ62は、ホームサーバ51の大容量記憶部68から読み出した個別鍵 $K_i$ をホームサーバ51の暗号処理部65に入力する。個別鍵 $K_i$ を受信した暗号処理部65は、暗号／復号化モジュール96の署名検証ユニット115で個別鍵 $K_i$ の署名を検証し、改竄がなされていないことが確認された場合には、ステップS167に進む。

ステップS167において、ホームサーバ51の上位コントローラ62は、ホームサーバ51の大容量記憶部68から読み出した取扱方針をホームサーバ51の暗号処理部65に入力する。取扱方針を受信した暗号処理部65は、暗号／復号化モジュール96の署名検証ユニット115で取扱方針の署名を検証し、改竄がなされていないことが確認された場合には、ステップS168に進む。ステップS168において、ホームサーバ51の上位コントローラ62は、ホームサーバ51の大容量記憶部68から読み出したサービスプロバイダ3の公開鍵証明書をホームサーバ51の暗号処理部65に入力する。

サービスプロバイダ3の公開鍵証明書を受信した暗号処理部65は、暗号／復号化モジュール96の署名検証ユニット115でサービスプロバイダ3の証明書の署名を検証した後、公開鍵証明書からサービスプロバイダ3の公開鍵を取り出す。署名の検証の結果、改竄がなされていないことが確認された場合には、ステップS169に進む。ステップS169において、ホームサーバ51の上位コン

トローラ 6 2 は、ホームサーバ 5 1 の大容量記憶部 6 8 から読み出した価格情報をホームサーバ 5 1 の暗号処理部 6 5 に入力する。価格情報を受信した暗号処理部 6 5 は、暗号／復号化モジュール 9 6 の署名検証ユニット 1 1 5 で価格情報の署名を検証し、改竄がなされていないことが確認された場合には、ステップ S 1 7 0 に進む。

ステップ S 1 7 0 において、ホームサーバ 5 1 の上位コントローラ 6 2 は、表示手段 6 4 を用いて購入可能なコンテンツの情報（例えば、購入可能な利用形態や価格など）を表示し、ユーザは入力手段 6 3 を用いて購入項目を選択する。入力手段 6 3 から入力された信号はホームサーバ 5 1 の上位コントローラ 6 2 に送信され、上位コントローラ 6 2 は、その信号に基づいて購入コマンドを生成し、購入コマンドをホームサーバ 5 1 の暗号処理部 6 5 に入力する。なお、これらの入力処理は購入処理スタート時に行っても良い。これを受信した暗号処理部 6 5 は、ステップ S 1 6 7 で入力された取扱方針およびステップ S 1 6 9 で入力された価格情報から課金情報および使用許諾条件情報を生成する。課金情報については、図 4 2 で説明したので、その詳細は省略する。使用許諾条件情報については、図 4 1 で説明したので、その詳細は省略する。

ステップ S 1 7 1 において、暗号処理部 6 5 の制御部 9 1 は、ステップ S 1 7 0 で生成した課金情報を記憶モジュール 9 2 に保存する。ステップ S 1 7 2 において、暗号処理部 6 5 の制御部 9 1 は、ステップ S 1 7 0 で生成した使用許諾条件情報を暗号処理部 6 5 の外部メモリ制御部 9 7 に送信する。使用許諾条件情報を受信した外部メモリ制御部 9 7 は、外部メモリ 6 7 の改竄チェックを行った後、使用許諾条件情報を外部メモリ 6 7 に書き込む。書き込む際の改竄チェックについては、図 6 9 を用いて後述する。ステップ S 1 7 3 において、暗号処理部 6 5 の制御部 9 1 は、ステップ S 1 6 6 で入力された個別鍵  $K_i$  を、暗号／復号化モジュール 9 6 の復号化ユニット 1 1 1 で、記憶モジュール 9 2 から供給された配送鍵  $K_d$  を用いて復号化する。次に、暗号処理部 6 5 の制御部 9 1 は、ステップ S 1 6 5 で入力されたコンテンツ鍵  $K_c$  を、暗号／復号化モジュール 9 6 の復

号化ユニット 111 で、先ほど復号化した個別鍵  $K_i$  を用いて復号化する。最後に、暗号処理部 65 の制御部 91 は、暗号／復号化モジュール 96 の暗号化ユニット 112 で、記憶モジュール 92 から供給された保存鍵  $K_{save}$  を用いてコンテンツ鍵  $K_c$  を暗号化する。ステップ S174 において、保存鍵  $K_{save}$  で暗号化されたコンテンツ鍵  $K_c$  は、暗号処理部 65 の外部メモリ制御部 97 を経由して外部メモリ 67 に保存される。

ステップ S162 でホームサーバ 51 が購入処理できない機器であると判定された場合、又はステップ S163 でコンテンツプロバイダ 2 の公開鍵証明書の署名が正しくないと判定された場合、又はステップ S164 でコンテンツ鍵  $K_c$  で暗号化されたコンテンツの署名が正しくないと判定された場合、又はステップ S165 で個別鍵  $K_i$  で暗号化されたコンテンツ鍵  $K_c$  の署名が正しくないと判定された場合、又はステップ S166 で配送鍵  $K_d$  で暗号化された個別鍵  $K_i$  の署名が正しくないと判定された場合、又はステップ S167 で取扱方針の署名が正しくないと判定された場合、又はステップ S168 でサービスプロバイダ 3 の証明書の署名が正しくないと判定された場合、又はステップ S169 で価格情報の署名が正しくないと判定された場合、ホームサーバ 51 はステップ S176 に進み、エラー処理を行う。なおステップ S165、およびステップ S166 の処理をまとめ、コンテンツ鍵  $K_c$ 、個別鍵  $K_i$  に対する唯一の署名を検証するようにしてもよい。

以上のように、ホームサーバ 51 は、課金情報を記憶モジュール 92 に記憶すると共に、コンテンツ鍵  $K_c$  を個別鍵  $K_i$  で復号化した後、コンテンツ鍵  $K_c$  を保存鍵  $K_{save}$  で暗号化し、外部メモリ 67 に記憶させる。

据置機器 52 も、同様の処理で、課金情報を暗号処理部 73 の記憶モジュールに記憶すると共に、コンテンツ鍵  $K_c$  を個別鍵  $K_i$  で復号化し、コンテンツ鍵  $K_c$  を保存鍵  $K_{save2}$  (ホームサーバ 51 の鍵と異なる) で暗号化し、外部メモリ 79 に記憶させる。

図 68 は、暗号処理部 65 の外部メモリ制御部 97 が、外部メモリ 67 からデ

ータを読み出す際に行う、改竄チェックの方法を説明するフローチャートである。図68のステップS180において、暗号処理部65の外部メモリ制御部97は、外部メモリ67から読み出すデータの場所を検索する（例えば図16の1ブロック目の1番目のデータ）。ステップS181において、暗号処理部65の外部メモリ制御部97は、外部メモリ67内の読み出し予定データを含む同一ブロック内全てのデータに対するハッシュ値（図16の1ブロック目全体のハッシュ値）を計算する。このとき、読み出し予定のデータ（例えばコンテンツ鍵1と使用許諾条件情報1）以外は、ハッシュ値計算に使用後、破棄される。ステップS182において、ステップS181で計算したハッシュ値と暗号処理部65の記憶モジュール92に記憶されているハッシュ値（ $ICV_1$ ）を比較する。一致していた場合、ステップS181で読み出しておいたデータを、外部メモリ制御部97を介して制御部91に送信し、一致していなかった場合、外部メモリ制御部97はステップS183に移り、当該メモリブロックは改竄されているものとして以降の読み書きを禁止する（不良ブロックとする）。例えば、外部メモリを4MBのフラッシュメモリとしたとき、このメモリを64のブロックに分けたものと仮定する。従って、記憶モジュールには64個のハッシュ値が記憶されている。データの読み出しを行う場合は、まず、データがある場所を検索し、そのデータを含む同一ブロック内の全てのデータに対するハッシュ値を計算する。このハッシュ値が、記憶モジュール内の当該ブロックに対応したハッシュ値と一致しているか否かで改竄をチェックする（図16参照）。

このように、暗号処理部65の外部メモリ制御部97は、外部メモリ67の改竄チェックを行い、データを読み出す。

図69は、暗号処理部65の外部メモリ制御部97が、外部メモリ67にデータを書き込む際に行う、改竄チェックの方法を説明するフローチャートである。図69のステップS190Aにおいて、暗号処理部65の外部メモリ制御部97は、外部メモリ67にデータを書き込むことができる場所を検索する。ステップS191Aにおいて、暗号処理部65の外部メモリ制御部97は、外部メモリ6

7内に空きエリアがあるか否か判定し、空きエリアがあると判定した場合、ステップS 1 9 2 Aに進む。ステップS 1 9 2 Aにおいて、暗号処理部6 5の外部メモリ制御部9 7は、書き込み予定データブロック内の、全てのデータに対するハッシュ値を計算する。ステップS 1 9 3 Aにおいて、ステップS 1 9 2 Aで計算したハッシュ値と暗号処理部6 5の記憶モジュール9 2に記憶されているハッシュ値を比較し、一致していた場合、ステップS 1 9 4 Aに進む。ステップS 1 9 4 Aにおいて、書き込み予定領域にデータを書き込む。ステップS 1 9 5 Aにおいて、暗号処理部6 5の外部メモリ制御部9 7は、書き込んだデータブロック内の、全てのデータに対するハッシュ値を再計算する。ステップS 1 9 6 Aにおいて、制御部9 1は、暗号処理部6 5の記憶モジュール9 2内のハッシュ値をステップS 1 9 5 Aで計算したハッシュ値に更新する。

ステップS 1 9 3 Aにおいて、計算したハッシュ値が記憶モジュール9 2内のハッシュ値と異なっていた場合、制御部9 1は、そのメモリブロックを不良ブロックとし（例えば、ハッシュ値を不良ブロックを示す値に変更する）、ステップS 1 9 0 Aへ進む。

ステップS 1 9 1 Aにおいて、外部メモリ6 7に空きエリアがないと判定された場合、ステップS 1 9 8 Aに進み、ステップS 1 9 8 Aにおいて、外部メモリ制御部9 7は、書き込みエラーを制御部9 1に返送し、処理を終了する。

外部メモリ制御部9 7の外部メモリ6 7への書き換え（更新）方法は、図7 0に示すように、ステップS 1 9 0 Bにおいて暗号処理部6 5の外部メモリ制御部9 7は、外部メモリ6 7のデータを書き換える場所を検索する。ステップS 1 9 2 Bにおいて、暗号処理部6 5の外部メモリ制御部9 7は、書き換え予定データブロック内の、全てのデータに対するハッシュ値を計算する。ステップS 1 9 3 Bにおいて、ステップS 1 9 2 Bで計算したハッシュ値と暗号処理部6 5の記憶モジュール9 2に記憶されているハッシュ値を比較し、一致していた場合、ステップS 1 9 4 Bに進む。ステップS 1 9 4 Bにおいて、書き換え予定領域のデータを書き換える。ステップS 1 9 5 Bにおいて、暗号処理部6 5の外部メモリ制

御部 97 は、書き込んだデータブロック内の、全てのデータに対するハッシュ値を再計算する。ステップ S 196 B において、制御部 91 は、暗号処理部 65 の記憶モジュール 92 内のハッシュ値をステップ S 195 B で計算したハッシュ値に更新する。

ステップ S 193 B において、計算したハッシュ値が記憶モジュール 92 内のハッシュ値と異なっていた場合、制御部 91 は、そのメモリブロックを不良ブロックとし（例えば、ハッシュ値を不良ブロックを示す値に変更する）、書き換え失敗とする。

外部メモリ 79 のデータの削除方法について、図 71 を用いて説明する。ステップ S 190 C において、暗号処理部 73 の外部メモリ制御部は、外部メモリ 79 のデータを削除する場所を検索する。ステップ S 192 C において、暗号処理部 73 の外部メモリ制御部は、データ削除予定データブロック内の、全てのデータに対するハッシュ値を計算する。ステップ S 193 C において、ステップ S 192 C で計算したハッシュ値と暗号処理部 73 の記憶モジュール（図示せず）に記憶されているハッシュ値を比較し、一致していた場合、ステップ S 194 C に進む。ステップ S 194 C において、削除予定領域の削除予定であるデータを削除する。ステップ S 195 C において、暗号処理部 73 の外部メモリ制御部は、削除予定データを削除したデータブロック内の、全てのデータに対するハッシュ値を再計算する。ステップ S 196 C において、暗号処理部 73 は記憶モジュール内のハッシュ値をステップ S 195 C で計算したハッシュ値に更新する。

ステップ S 193 C において、計算したハッシュ値が記憶モジュール内のハッシュ値と異なっていた場合、暗号処理部 73 は、そのメモリブロックを不良ブロックとし（例えば、ハッシュ値を不良ブロックを示す値に変更する）、消去失敗とする。

図 56 のステップ S 46 に対応するホームサーバ 51 がコンテンツを再生する処理の詳細を、図 72 及び図 73 のフローチャートを用いて説明する。ステップ S 200 において、ホームサーバ 51 の上位コントローラ 62 は、ホームサーバ

51の入力手段63から再生指示されたコンテンツに対応するIDを、ホームサーバ51の暗号処理部65に入力する。ステップS201において、再生するコンテンツIDを受信した暗号処理部65の制御部91は、コンテンツIDを暗号処理部65の外部メモリ制御部97に送信し、コンテンツIDに対応するコンテンツ鍵 $K_c$ および使用許諾条件情報を検索させる。このとき、使用許諾条件情報が再生可能な権利であることを確認する。ステップS202において、暗号処理部65の外部メモリ制御部97は、コンテンツ鍵 $K_c$ および使用許諾条件情報を含むデータブロックのハッシュ値を計算し、暗号処理部65の制御部91に送信する。ステップS203において、暗号処理部65の制御部91は、暗号処理部65の記憶モジュール92に記憶されているハッシュ値とステップS202で受信したハッシュ値が一致しているか否か判定し、一致していた場合にはステップS204に進む。

ステップS204において、暗号処理部65の制御部91は、使用許諾条件情報を必要に応じて更新する。例えば、使用許諾条件情報内の利用権が回数券であった場合、その回数を減算するなどの処理である。従って、更新する必要のない買い切りの権利などは、更新する必要がなく、その場合、ステップS208へジャンプする（図示していない）。ステップS205において、外部メモリ制御部97は、制御部91から送信された更新された使用許諾条件情報を、外部メモリ67に書き換え更新する。ステップS206において、外部メモリ制御部97は、書き換えたデータブロック内の全データに対するハッシュ値を計算し直し、暗号処理部65の制御部91に送信する。ステップS207において、暗号処理部65の制御部91は、暗号処理部65の記憶モジュール92に記憶されているハッシュ値を、ステップS206で算出したハッシュ値に書き換える。

ステップS208において、暗号処理部65と伸張部66は相互認証を行い、一時鍵 $K_{temp}$ を共有する。相互認証処理は、図51を用いて説明したのでその詳細は省略する。ステップS209において、暗号／復号化モジュール96の復号化ユニット111は、外部メモリ97から読み出したコンテンツ鍵 $K_c$ を、記憶モ

ジュール 9 2 から供給された保存鍵  $K_{save}$  で復号化する。ステップ S 2 1 0 において、暗号／復号化モジュール 9 6 の暗号化ユニット 1 1 2 は、先ほど伸張部 6 6 と共有した一時鍵  $K_{temp}$  でコンテンツ鍵  $K_c$  を再暗号化する。ステップ S 2 1 1 において、暗号処理部 6 5 の制御部 9 1 は、上位コントローラ 6 2 を介して、一時鍵  $K_{temp}$  で暗号化されたコンテンツ鍵  $K_c$  を伸張部 6 6 に送信する。

ステップ S 2 1 2 において、伸張部 6 6 の鍵復号モジュール 1 0 2 は、相互認証モジュール 1 0 1 から供給された一時鍵  $K_{temp}$  でコンテンツ鍵  $K_c$  を復号化する。ステップ S 2 1 3 において、上位コントローラ 6 2 は大容量記憶部 6 8 からコンテンツを読み出し、伸張部 6 6 に供給する。コンテンツを受信した伸張部 6 6 の復号モジュール 1 0 3 は、鍵復号モジュール 1 0 2 から供給されたコンテンツ鍵  $K_c$  を用いてコンテンツを復号化する。ステップ S 2 1 4 において、伸張部 6 6 の伸張モジュール 1 0 4 は、コンテンツを所定の方式、例えば ATRAC などの方式により伸張する。ステップ S 2 1 5 において、電子透かし付加モジュール 1 0 5 は、暗号処理部 6 5 から指示されたデータを電子透かしの形でコンテンツに挿入する（暗号処理部から伸張部へ渡されるデータは、コンテンツ鍵  $K_c$  だけではなく、再生条件（アナログ出力、デジタル出力、コピー制御信号付き出力（SCMS）、コンテンツ利用権を購入した機器 ID など）も含まれている。挿入するデータは、このコンテンツ利用権を購入した機器の ID（つまりは、使用許諾条件情報内の機器 ID）などである）。ステップ S 2 1 6 において、伸張部 6 6 は、図示せぬスピーカを介して音楽を再生する。

このように、ホームサーバ 5 1 は、コンテンツを再生する。

図 7 4 は、ホームサーバ 5 1 が据置機器 5 2 のために、コンテンツ利用権を代理購入する処理の詳細を説明したフローチャートである。ステップ S 2 2 0 において、ホームサーバ 5 1 と据置機器 5 2 は、相互認証する。相互認証処理は、図 5 2 で説明した処理と同様なため、説明を省略する。ステップ S 2 2 1 において、ホームサーバ 5 1 の上位コントローラ 6 2 は、ホームサーバ 5 1 の大容量記憶部 6 8 から読み出した登録情報を、ホームサーバ 5 1 の暗号処理部 6 5 に検査さ



せる。上位コントローラ 6 2 から登録情報を受信した暗号処理部 6 5 は、暗号／復号化モジュール 9 6 の署名検証ユニット 1 1 5 に、登録情報に付加されている署名を、暗号処理部 6 5 の記憶モジュール 9 2 から供給された電子配信サービスセンタ 1 の公開鍵で検証させる。署名の検証に成功した後、暗号処理部 6 5 の制御部 9 1 は、登録情報に据置機器の ID が登録され、「登録」及び「購入」の項目が「登録可」及び「購入化」になっているか判定し、「登録可」になっていると判定された場合にはステップ S 2 2 2 に進む（なお、据置機器 5 2 側でも登録情報を検査し、ホームサーバ 5 1 が「登録可」になっていることを判定している）。ステップ S 2 2 5 からステップ S 2 2 7 は、図 6 7 のステップ S 1 6 0 からステップ S 1 7 1 までと同様な処理のため、その詳細は省略する。

ステップ S 2 2 8 において、暗号処理部 6 5 の制御部 9 1 は、ステップ S 2 2 5 で入力された配送鍵  $K_d$  で暗号化された個別鍵  $K_i$  を、暗号／復号化モジュール 9 6 の復号化ユニット 1 1 1 で、記憶モジュール 9 2 から供給された配送鍵  $K_d$  を用いて復号化する。次に、暗号処理部 6 5 の制御部 9 1 は、ステップ S 2 2 5 で入力された個別鍵  $K_i$  で暗号化されたコンテンツ鍵  $K_{co}$  を、暗号／復号化モジュール 9 6 の復号化ユニット 1 1 1 で、個別鍵  $K_i$  を用いて復号化する。そして、暗号処理部 6 5 の制御部 9 1 は、暗号／復号化モジュール 9 6 の暗号化ユニット 1 1 2 で、ステップ S 2 2 0 の相互認証時に据置機器 5 2 と共有した一時鍵  $K_{temp}$  を用いてコンテンツ鍵  $K_{co}$  を再暗号化する。ステップ S 2 2 9 において、暗号処理部 6 5 の制御部 9 1 は、一時鍵  $K_{temp}$  で暗号化されたコンテンツ鍵  $K_{co}$  と、ステップ S 2 2 6 で生成した使用許諾条件情報に対し、暗号／復号化モジュール 9 6 の署名生成ユニット 1 1 4 を用いて署名を生成し、上位コントローラ 6 2 に送信する。一時鍵  $K_{temp}$  で暗号化されたコンテンツ鍵  $K_{co}$ 、使用許諾条件情報およびそれらの署名を受信したホームサーバ 5 1 の上位コントローラ 6 2 は、大容量記憶部 6 8 からコンテンツ鍵  $K_{co}$  で暗号化されたコンテンツ（署名を含む。以下同じ）を読み出し、一時鍵  $K_{temp}$  で暗号化されたコンテンツ鍵  $K_{co}$ 、使用許諾条件情報、それらの署名およびコンテンツ鍵  $K_{co}$  で暗号化されたコンテンツを据置機器

52に送信する。

ステップS230において、一時鍵 $K_{temp}$ で暗号化されたコンテンツ鍵 $K_{co}$ 、使用許諾条件情報、それらの署名およびコンテンツ鍵 $K_{co}$ で暗号化されたコンテンツを受信した据置機器52は、署名を検証した後コンテンツ鍵 $K_{co}$ で暗号化されたコンテンツを据置機器52の記録再生部76に出力する。コンテンツ鍵 $K_{co}$ で暗号化されたコンテンツを受信した据置機器52の記録再生部76は、コンテンツ鍵 $K_{co}$ で暗号化されたコンテンツを記録メディア80に保存する。

ステップS231において、据置機器52の暗号処理部73は、一時鍵 $K_{temp}$ で暗号化されたコンテンツ鍵 $K_{co}$ を、暗号／復号化モジュールの復号化ユニットで、ステップS220の相互認証時にホームサーバ51と共有した一時鍵 $K_{temp}$ を用いて復号化する。そして、暗号処理部73の制御部は、暗号／復号化モジュールの暗号化ユニットで、暗号処理部73の記憶モジュールから供給された保存鍵 $K_{save2}$ を用いてコンテンツ鍵 $K_{co}$ を再暗号化する。

ステップS232において、据置機器52の暗号処理部73は、保存鍵 $K_{save2}$ で暗号化されたコンテンツ鍵 $K_{co}$ とステップS230で受信した使用許諾条件情報を暗号処理部73の外部メモリ制御部に送信し、外部メモリ79に保存させる。外部メモリ制御部が外部メモリにデータを書き込む処理については、図69で説明しているので、詳細は省略する。

このように、ホームサーバ51はコンテンツ利用権を購入し、課金情報はホームサーバ51側で保存し、利用権は据置機器52に引き渡される。

図75は、ホームサーバ51が、既に購入済みのコンテンツ利用権を、別の利用形態に変更して購入するための処理を示したフローチャートである。図75のステップS240からステップS245までは、図67で説明した処理と同様であるため、その説明は省略する。ステップS246において、ホームサーバ51の暗号処理部65は、暗号処理部65の外部メモリ制御部97に、利用権変更するコンテンツの使用許諾条件情報を読み出させる。外部メモリ67からのデータの読み出しは、図68を参照して説明したので、その詳細は省略する。ステップ

S 2 4 6 で正常に使用許諾条件情報が読み出せた場合には、ステップ S 2 4 7 へ進む。

ステップ S 2 4 7 において、ホームサーバ 5 1 の上位コントローラ 6 2 は、表示手段 6 4 を用いて利用権内容変更可能なコンテンツの情報（例えば、利用権内容変更可能な利用形態や価格など）を表示し、ユーザは入力手段 6 3 を用いて利用権内容更新条件を選択する。入力手段 6 3 から入力された信号はホームサーバ 5 1 の上位コントローラ 6 2 に送信され、上位コントローラ 6 2 は、その信号に基づいて利用権内容変更コマンドを生成し、利用権内容変更コマンドをホームサーバ 5 1 の暗号処理部 6 5 に入力する。これを受信した暗号処理部 6 5 は、ステップ S 2 4 3 で受信した取扱方針、ステップ S 2 4 5 で受信した価格情報およびステップ S 2 4 7 で読み出した使用許諾条件情報から、課金情報および新しい使用許諾条件情報を生成する。

ステップ S 2 4 8 は、図 6 7 のステップ S 1 7 1 と同様なため、その詳細な説明は省略する。ステップ S 2 4 9 において、暗号処理部 6 5 の制御部 9 1 は、ステップ S 2 4 7 で生成した使用許諾条件情報を、暗号処理部 6 5 の外部メモリ制御部 9 7 に出力する。外部メモリ制御部 9 7 は、受信した使用許諾条件情報を外部メモリ 6 7 に上書き更新する。外部メモリ制御部 9 7 の外部メモリ 6 7 への書き換え（更新）方法は、図 7 0 で説明したので、その詳細は省略する。

ステップ S 2 4 6 において、外部メモリ 6 7 に、権利内容変更コマンドに付加されたコンテンツ ID に対応する使用許諾条件情報が見つからなかった場合、または、使用許諾条件情報が記憶されている外部メモリの記憶ブロックに改竄が発見された場合（図 6 8 を参照して説明済み）、ステップ S 2 5 1 へ進み、所定のエラー処理を行う。

このように、ホームサーバ 5 1 は、既に購入した権利（使用許諾権条件情報に記述されている）と、取扱方針および価格情報を用いて新たな権利を購入し、利用権内容を変更することができる。

図 7 6 及び図 7 7 は、取扱方針および価格情報のルール部分の具体例を示した

ものである。図 7 6 において、取扱方針は利用権ごとに整理番号として付けられたルール番号、利用権内容を示す利用権内容番号、そのパラメータ、最低販売価格、コンテンツプロバイダの利益率から構成され、この取扱方針には例えば 5 つのルールが記述されている。ルール 1 は、権利項目が利用権内容番号 1 であるから、図 4 4 より、その権利は再生権、時間・回数制限なしの権利であることがわかる。また、パラメータの項目には、特に記述がないことがわかる。最低販売価格は ¥ 3 5 0 であり、コンテンツプロバイダ 2 の取り分は、価格の 3 0 % である。ルール 2 は、権利項目が利用権内容番号 2 であるから、図 4 4 より、その権利は再生権、時間制限有り、回数制限なしの権利であることがわかる。また、利用可能期間が 1 時間であることが、パラメータの項目からわかる。最低販売価格は ¥ 1 0 0 であり、コンテンツプロバイダ 2 の取り分は、価格の 3 0 % である。ルール 3 は、権利項目が利用権内容番号 6 であるから、図 4 4 より、その権利は複製権（コピー制御信号なし）、時間制限なし、回数制限ありの権利であることがわかる。また、利用可能回数が 1 回であることが、パラメータの項目からわかる。最低販売価格は ¥ 3 0 であり、コンテンツプロバイダ 2 の取り分は、価格の 3 0 % である。

ルール 4 は、権利項目が利用権内容番号 1 3 であるから、図 4 4 より、その権利は利用内容変更であることがわかる。変更可能なルール番号は、# 2（再生権、時間制限有り、回数制限なし）から # 1（再生権、時間・回数制限なし）であることがパラメータの項目からわかる。最低販売価格は ¥ 2 0 0 であり、コンテンツプロバイダ 2 の取り分は、価格の 2 0 % である。最低販売価格がルール 1 より低く提示してあるのは、既に購入している権利を下取りして再購入すると考えているからであり、コンテンツプロバイダ 2 の取り分がルール 1 より低く提示してあるのは、実際の作業をする電子配信サービスセンタ 1 の取り分を増やすためである（コンテンツプロバイダ 2 は、権利内容変更時には作業がないため）。

ルール 5 は、権利項目が利用権内容番号 1 4 であるから、図 4 4 より、その権利は再配布であることがわかる。再配布可能条件は、ルール番号 # 1（再生権、

時間・回数制限なし)を持っている機器が、ルール番号#1(再生権、時間・回数制限なし)を購入して再配布することであることが、パラメータの項目からわかる。最低販売価格は¥250であり、コンテンツプロバイダ2の取り分は、価格の20%である。最低販売価格がルール1より低く提示してあるのは、既に購入している権利をもつ機器が、同一コンテンツにつき再購入すると考えているからであり、コンテンツプロバイダ2の取り分がルール1より低く提示してあるのは、実際の作業をする電子配信サービスセンタ1の取り分を増やすためである(コンテンツプロバイダ2は、再配付時には作業がないため)。

図77において、価格情報は利用権ごとに整理番号として付けられたルール番号、パラメータ及び価格情報から構成され、この価格情報にも例えば5つのルールが記述されている。ルール1は、取扱方針のルール#1に対する価格情報で、利用権内容番号#1を購入する際に、価格が¥500で、サービスプロバイダ3の取り分が30%であることを示す。従って、ユーザが支払う¥500は、コンテンツプロバイダ2が¥150、サービスプロバイダ3が¥150、電子配信サービスセンタ1が¥200取ることになる。ルール2からルール5までも同様であるので、その詳細は省略する。

なお、ルール4、5において、サービスプロバイダ2の取り分がルール1に比べて少ないのは、サービスプロバイダ2の配信作業をユーザ機器が代行して行っており、代金の回収は電子配信サービスセンタ1が行っているためである。

また本例ではルール番号が#1から#5へと連番となっているが、必ずしもその必要はない。作成者はルール番号ごとに利用権内容番号とパラメータを設定しておき、そこから抽出したものを並べるため、一般には連番にならない。

図78は、図75で説明した権利内容変更を行う際の具体的な例を示したものである。取扱方針は利用権ごとに整理番号として付けられたルール番号、利用権内容を示す利用権内容番号、そのパラメータ、最低販売価格、コンテンツプロバイダの利益率から構成され、価格情報は利用権ごとに整理番号として付けられたルール番号、パラメータ及び価格情報から構成され、使用許諾条件情報は利用権

ごとに整理番号として付けられたルール番号、利用権内容を示す利用権内容番号、そのパラメータから構成されている。ホームサーバ51は、既にルール番号#2の再生権、時間制限ありの権利を購入しており、権利内容を示す使用許諾条件情報には、ルール番号#2が記述されており、利用可能時間は残り30分で、今まで積算して2時間分の購入を行っていることを示している。今、時間制限ありから時間制限なしに変更しようとした場合、取扱方針のルール3、価格情報のルール3および使用許諾条件情報から¥200で再生権、時間・回数制限なしに変更でき、使用許諾条件情報は、ルール番号#1、利用権内容番号の再生権、時間・回数制限なしに変わることがわかる（利用権内容番号#1の場合のパラメータに関しては、後述する。また、本例で言えば、直接再生権、時間・回数制限なしを買う場合に比べ、一度、時間制限ありの権利を買ってから権利内容変更したほうが安くなってしまっている。このため、積算利用時間を見て割り引くようにした方がよい）。

図79は、ホームサーバ51が据置機器52のために、コンテンツ利用権を購入し、その利用権を再配布する処理の詳細を説明したフローチャートである。ステップS260からステップ264は、図74のステップS220からステップS225と同様なため、その詳細な説明は省略する。ステップS265において、ホームサーバ51の暗号処理部65は、暗号処理部65の外部メモリ制御部97に、再配布しようとするコンテンツに対応する使用許諾条件情報および保存鍵 $K_{save}$ で暗号化されたコンテンツ鍵 $K_c$ を、外部メモリ67から読み出させる。外部メモリ制御部97による外部メモリ67の読み出し方法については、図68で説明したので、その詳細は省略する。読み出しに成功した場合は、ステップS266に進む。

ステップS266において、ホームサーバ51の上位コントローラ62は、表示手段64を用いて再配布可能なコンテンツの情報（例えば、再配布可能なコンテンツの利用形態や価格など）を表示し、ユーザは入力手段63を用いて再配付条件を選択する。なお、この選択処理は、予め再配付処理スタート時に行うよう

にしても良い。入力手段 6 3 から入力された信号はホームサーバ 5 1 の上位コントローラ 6 2 に送信され、上位コントローラ 6 2 は、その信号に基づいて再配布コマンドを生成し、再配布コマンドをホームサーバ 5 1 の暗号処理部 6 5 に入力する。これを受信した暗号処理部 6 5 は、ステップ S 2 6 4 で受信した取扱方針、価格情報およびステップ S 2 6 5 で読み出した使用許諾条件情報から、課金情報および新しい使用許諾条件情報を生成する。

ステップ S 2 6 7 は、図 6 7 のステップ S 1 7 1 と同様なため、その詳細な説明は省略する。ステップ S 2 6 8 において、暗号処理部 6 5 の制御部 9 1 は、ステップ S 2 6 5 で読み出した保存鍵  $K_{save}$  で暗号化されたコンテンツ鍵  $K_{co}$  を、暗号／復号化モジュール 9 6 の復号化ユニット 1 1 1 で、記憶モジュール 9 2 から供給された保存鍵  $K_{save}$  を用いて復号化する。そして、暗号処理部 6 5 の制御部 9 1 は、暗号／復号化モジュール 9 6 の暗号化ユニット 1 1 2 で、ステップ S 2 6 0 の相互認証時に据置機器 5 2 と共有した一時鍵  $K_{temp}$  を用いてコンテンツ鍵  $K_{co}$  を再暗号化する。最後に、暗号／復号化モジュール 9 6 の署名生成ユニット 1 1 4 は、一時鍵  $K_{temp}$  で暗号化されたコンテンツ鍵  $K_{co}$  と、ステップ S 2 6 6 で生成した新しい使用許諾条件情報に対応した署名を生成し、暗号処理部 6 5 の制御部 9 1 に返送する。

ステップ S 2 6 9 からステップ S 2 7 2 の処理は、図 7 4 のステップ S 2 2 9 からステップ S 2 3 2 と同様なため、その詳細は省略する。

このように、ホームサーバ 5 1 は、自己の保持する利用権（使用許諾条件情報）と取扱方針、価格情報から新しい使用許諾条件情報を作り出し、自己の保持するコンテンツ鍵  $K_{co}$ 、コンテンツとともに据置機器 5 2 へ送信することで、コンテンツの再配布が行える。

図 8 0 は、ホームサーバ 5 1 が据置機器 5 2 のために、使用許諾条件情報、コンテンツ鍵  $K_{co}$  を送信し、据置機器 5 2 でコンテンツ利用権を購入する処理の詳細を説明したフローチャートである。ステップ S 2 8 0 において、据置機器 5 2 の暗号処理部 7 3 は、暗号処理部 7 3 の記憶モジュールに記憶されている課金情

報の課金の合計が、上限に達しているか否か判定し、上限に達していなかった場合にはステップS 2 8 1に進む（なお、課金合計上限で判定するのではなく、課金処理件数の上限で判定するようにしても良い）。

ステップS 2 8 1において、据置機器5 2の上位コントローラ7 2は、据置機器5 2の小容量記憶部7 5から読み出した登録情報を据置機器5 2の暗号処理部7 3に入力する。登録情報を受信した暗号処理部7 3は、図示せぬ暗号／復号化モジュールの署名検証ユニットで登録情報の署名を検証した後、据置機器5 2のIDに対する「購入処理」の項目が「購入可」になっているか判定し、「購入可」であった場合にはステップS 2 8 2に進む。

ステップS 2 8 2は、図7 4のステップS 2 2 0と同様なため、その詳細は省略する。ステップS 2 8 3は、図7 4のステップS 2 2 1と同様なため、その詳細は省略する（ホームサーバ5 1は据置機器5 2が登録されているか否かを判定し、据置機器5 2はホームサーバ5 1が登録されているか否かを判定する）。ステップS 2 8 4は、図7 9のステップS 2 6 5と同様なため、その詳細は省略する。ステップS 2 8 5は、図7 9のステップS 2 6 8と同様なため、その詳細は省略する。ステップS 2 8 6において、暗号処理部6 5の制御部9 1は、一時鍵 $K_{temp}$ で暗号化されたコンテンツ鍵 $K_{co}$ と、ステップS 2 8 4で読み出した使用許諾条件情報に対し、暗号／復号化モジュール9 6の署名生成ユニット1 1 4を用いて署名を生成し、上位コントローラ6 2に送信する。一時鍵 $K_{temp}$ で暗号化されたコンテンツ鍵 $K_{co}$ 、使用許諾条件情報およびそれらの署名を受信したホームサーバ5 1の上位コントローラ6 2は、大容量記憶部6 8からコンテンツ鍵 $K_{co}$ で暗号化されたコンテンツ、必要に応じて取扱方針とその署名、価格情報とその署名を読み出し、一時鍵 $K_{temp}$ で暗号化されたコンテンツ鍵 $K_{co}$ 、使用許諾条件情報、それらの署名、コンテンツ鍵 $K_{co}$ で暗号化されたコンテンツ、取扱方針とその署名および価格情報とその署名を据置機器5 2に送信する。

ステップS 2 8 7は、図7 4のステップS 2 3 0と同様なため、その詳細は省略する。ステップS 2 8 8は、図7 4のステップS 2 2 5と同様なため、その詳



細は省略する。ステップS 2 8 9において、据置機器5 2の上位コントローラ7 2は、表示手段7 8を用いて再配布可能なコンテンツの情報（例えば、再配布可能なコンテンツの利用形態や価格など）を表示し、ユーザは入力手段7 7を用いて再配付条件を選択する。なお、この選択処理は予め再配付処理スタート時に行うようにしても良い。入力手段7 7から入力された信号は据置機器5 2の上位コントローラ7 2に送信され、上位コントローラ7 2は、その信号に基づいて再配布コマンドを生成し、再配布コマンドを据置機器5 2の暗号処理部7 3に入力する。これを受信した暗号処理部7 3は、ステップS 2 8 6で受信した取扱方針、価格情報および使用許諾条件情報から、課金情報および新しい使用許諾条件情報を生成する。

ステップS 2 9 0において、据置機器5 2の暗号処理部7 3は、ステップS 2 8 9で生成した課金情報を暗号処理部7 3の図示せぬ記憶モジュールに保存する。ステップS 2 9 1において、据置機器5 2の暗号処理部7 3は、ステップS 2 8 6で受信した一時鍵 $K_{temp}$ で暗号化されたコンテンツ鍵 $K_{co}$ を、暗号処理部7 3の図示せぬ復号化ユニットで、ステップS 2 8 2で共有した一時鍵 $K_{temp}$ を用いて復号化する。そして、据置機器5 2の暗号処理部7 3は、暗号処理部7 3の図示せぬ暗号化ユニットで、暗号処理部7 3の図示せぬ記憶モジュールから供給された保存鍵 $K_{save2}$ を用いてコンテンツ鍵 $K_{co}$ を暗号化する。

ステップS 2 9 2において、据置機器5 2の暗号処理部7 3は、ステップS 2 8 9で生成した使用許諾条件情報およびステップS 2 9 1で生成した保存鍵 $K_{save2}$ で暗号化されたコンテンツ鍵 $K_{co}$ を暗号処理部7 3の図示せぬ外部メモリ制御部に送信する。使用許諾条件情報および保存鍵 $K_{save2}$ で暗号化されたコンテンツ鍵 $K_{co}$ を受信した外部メモリ制御部は、使用許諾条件情報および保存鍵 $K_{save2}$ で暗号化されたコンテンツ鍵 $K_{co}$ を外部メモリ7 9に書き込む。書き込む際の改竄チェックについては、図6 9を用いて説明したので、その詳細は省略する。

このように、据置機器5 2は、ホームサーバ5 1の保持する利用権（使用許諾条件情報）、取扱方針、価格情報、コンテンツ鍵 $K_{co}$ 、コンテンツをホームサーバ

5 1 から受信し、据置機器 5 2 で新しい使用許諾条件情報を作り出すことにより、コンテンツの再配布を受けることができる。

図 8 1 は、管理移動権について説明した図である。管理移動とは、機器 1 から機器 2 へ再生権を移動できる動作のことで、機器 1 から機器 2 へ権利が移動することは通常の移動と同じであるが、機器 2 は受け取った再生権を再移動することができない点で通常の移動と異なる（通常の移動と同様に、再生権を移動した後の機器 1 は、再生権の再移動できない）。再生権を管理移動で受け取った機器 2 は、再生権を機器 1 に返還することができ、返還された後は、機器 1 は再度再生権の移動ができ、機器 2 は引き続きできない。これらを実現するため、使用許諾条件情報に管理移動権の購入者および現在の管理移動権の保持者を管理させている（ここでは、利用権内容番号 # 1 を持っている場合にのみ管理移動できることを想定しているが、利用権内容番号 # 2 においても拡張できる）。

図 8 1 において、取扱方針のルール 1 は、図 7 8 で説明しているので、その詳細は省略する。ルール 2 は、権利項目が利用権内容番号 1 6 であるから、図 4 4 より、その権利は管理移動権であることがわかる。また、パラメータの項目には、特に記述がないことがわかる。最低販売価格は ¥ 1 0 0 であり、コンテンツプロバイダ 2 の取り分は、価格の 5 0 % である。コンテンツプロバイダ 2 の取り分がルール 1 より高く提示してあるのは、サービスプロバイダ 3 は実際の作業を全く行わないため、その分をコンテンツプロバイダ 2 への取り分に回したためである。

図 8 1 において、価格情報のルール 1 は、図 7 8 で説明しているので、その詳細は省略する。ルール 2 は、取扱方針のルール # 2 に対する価格情報で、利用権内容番号 # 1 6 を購入する際に、価格が ¥ 1 0 0 で、サービスプロバイダ 3 の取り分が 0 % であることを示す。従って、ユーザが支払う ¥ 1 0 0 は、コンテンツプロバイダ 2 が ¥ 5 0、サービスプロバイダ 3 が ¥ 0、電子配信サービスセンタ 1 が ¥ 5 0 取ることになる。

図 8 1 において、ユーザはまずルール番号 # 1（再生権、時間・回数制限無し

）を購入する。ただし、このとき管理移動権は持っていない（図 8 1 の a の状態）。次に、ユーザは管理移動権を購入する（これらの動作は一瞬のため、ユーザは一括して購入したように見える）。使用許諾条件のルール番号は、購入者を示す暗号処理部の ID（以下購入者とする）が ID 1（例えば、ホームサーバ 5 1 の ID）、再生権を保有する暗号処理部の ID（以下保持者とする）が ID 2 になる（図 8 1 の b の状態）。これを、管理移動を行って据置機器 5 2 に移した場合、ホームサーバ 5 1 の持つ使用許諾条件情報のルール部は、購入者は ID 1 のままだが、保持者が ID 2 に変化する。また、管理移動により再生権を受信した据置機器 5 2 の持つ使用許諾条件情報のルール部は、購入者は ID 1、保持者は ID 2 となり、ホームサーバ 5 1 の使用許諾条件情報と一緒にになっている。

図 8 2 は、管理移動権の移動処理の詳細を説明するフローチャートである。図 8 2 において、ステップ S 3 0 0 は、図 7 4 のステップ S 2 2 0 と同様のため、その詳細は省略する。また、ステップ S 3 0 1 は図 7 4 のステップ S 2 2 1 と同様のため、その詳細は省略する。ステップ S 3 0 2 は図 7 5 のステップ S 2 4 6 と同様であるため、その詳細は省略する。ステップ S 3 0 3 において、ホームサーバ 5 1 の暗号処理部 6 5 は、読み出した使用許諾条件情報内のルール部を検査し、使用権が再生権、時間・回数制限なし、管理移動権ありになっているか判定する。管理移動権があると判定された場合、ステップ S 3 0 4 に進む。

ステップ S 3 0 4 において、暗号処理部 6 5 の制御部 9 1 は、管理移動権の購入者および保持者が、共にホームサーバ 5 1 の ID になっているか判定する。管理移動権の購入者および保持者が、共にホームサーバ 5 1 の ID になっていると判定された場合には、ステップ S 3 0 5 に進む。ステップ S 3 0 5 において、暗号処理部 6 5 の制御部 9 1 は、使用許諾条件情報の管理移動権の保持者を据置機器 5 2 の ID に書き換える。ステップ S 3 0 6 において、暗号処理部 6 5 の制御部 9 1 は、ステップ S 3 0 5 で書き換えた使用許諾条件情報を暗号処理部 6 5 の外部メモリ制御部 9 7 に出力する。使用許諾条件情報を受信した暗号処理部 6 5 の外部メモリ制御部 9 7 は、外部メモリ 6 7 に使用許諾条件情報を上書き保存す

る。外部メモリ 67 のデータを書き換え保存する方法については、図 70 で説明したので、その詳細は省略する。ステップ S 307 からステップ S 311 までは、図 79 のステップ S 268 からステップ S 272 と同様なため、その詳細は省略する。

ステップ S 303 で使用許諾条件情報に管理移動権が含まれていなかった場合、ステップ S 304 で管理移動権の購入者または保持者がホームサーバ 51 でなかった場合は、処理を中断する。

このように、ホームサーバ 51 から据置機器 52 にコンテンツを再生するための権利を移動することができる。

図 83 は、現在管理移動権を所持している据置機器 52 から、管理移動権の購入者であるホームサーバ 51 に、管理移動権を返還させる処理について説明したフローチャートである。図 83 において、ステップ S 320 は、図 74 のステップ S 220 と同様なため、その詳細は省略する。ステップ S 321 は図 74 のステップ S 221 と同様であるため、その詳細は省略するが、ホームサーバ 51 と据置機器 52 双方で相手の ID が登録されているか検査しているものとする。登録されていると判定された場合、ステップ S 322 に進む。ステップ S 322 は、図 75 のステップ S 246 と同様であるため、その詳細は省略するが、ホームサーバ 51 と据置機器 52 双方で同一のコンテンツ ID のデータを読み出していることとする。外部メモリからデータが正しく読めた場合には、ステップ S 323 に進む。ステップ S 323 は、図 82 のステップ S 303 と同様であるため、その詳細は省略するが、ホームサーバ 51 と据置機器 52 双方で管理移動権があるか判定していることとする。管理移動権があると判定された場合には、ステップ S 324 に進む。

ステップ S 324 において、ホームサーバ 51 の暗号処理部 65 は、管理移動権の購入者がホームサーバ 51 の ID になっていて、保持者が据置機器 52 の ID になっているか判定する。管理移動権の購入者がホームサーバ 51 の ID になっていて、保持者が据置機器 52 の ID になっていると判定された場合には、ス

ステップS 3 2 5に進む。同様に、据置機器 5 2 の暗号処理部 7 3 は、管理移動権の購入者がホームサーバ 5 1 の I D になっていて、保持者が据置機器 5 2 の I D になっているか判定する。管理移動権の購入者がホームサーバ 5 1 の I D になっていて、保持者が据置機器 5 2 の I D になっていると判定された場合には、ステップS 3 2 5に進む。

ステップS 3 2 5において、据置機器 5 2 の記録再生部 7 6 は、記録メディア 8 0 からコンテンツを削除する（ただし、暗号化されたデータが残るだけなので、無理に削除する必要はない）。ステップS 3 2 6において、据置機器 5 2 の暗号処理部 7 3 は、暗号処理部 7 3 の図示せぬ外部メモリ制御部に、外部メモリ 7 9 に保存されている保存鍵  $K_{save2}$  で暗号化されたコンテンツ鍵  $K_{co}$  と使用許諾条件情報を削除させる。外部メモリ 7 9 の照りの削除方法は図 7 1 で説明したので、その詳細は省略する。

ステップS 3 2 7において、暗号処理部 6 5 の制御部 9 1 は、使用許諾条件情報の管理移動権の保持者をホームサーバ 5 1 の I D に書き換えた使用許諾条件情報を生成する。ステップS 3 2 8において、暗号処理部 6 5 の制御部 9 1 は、ステップS 3 2 7で生成した使用許諾条件情報を、暗号処理部 6 5 の外部メモリ制御部 9 7 に出力する。使用許諾条件情報を受信した暗号処理部 6 5 の外部メモリ制御部 9 7 は、外部メモリ 6 7 に使用許諾条件情報を上書き保存する。外部メモリ 6 7 に書き換え保存する方法については、図 7 0 で説明したので、その詳細は省略する。

ステップS 3 2 1でホームサーバ 5 1 または据置機器 5 2 において、登録情報が改竄されていたり、相手の機器の I D が登録されていなかった場合、ステップS 3 2 2でホームサーバ 5 1 または据置機器 5 2 において、外部メモリ内に所定のコンテンツに対するコンテンツ鍵または使用許諾条件情報が見つからなかったり、それらを含むメモリブロックが改竄されていた場合は、ステップS 3 2 9へ進みエラー処理を行う。

ステップS 3 2 3でホームサーバ 5 1 または据置機器 5 2 において、使用許諾

条件情報内に管理移動権がなかった場合、ステップS 3 2 4でホームサーバ5 1または据置機器5 2において、購入者がホームサーバ5 1で、保持者が据置機器5 2でなかった場合は、処理を中断する。

このように、据置機器5 2からホームサーバ5 1にコンテンツを再生するための権利をもどすことができる。

なお、コンテンツおよびコンテンツ鍵 $K_c$ 等を1つしか記述していないが、必要に応じて複数存在することとする。

また、本例ではコンテンツプロバイダ2とサービスプロバイダ3が別々に扱われていたが、一つにまとめてしまってもよい。更にまた、コンテンツプロバイダ2の方式を、そのままサービスプロバイダ3に転用しても良い。

## (2) 個別鍵の使用による暗号化处理

コンテンツプロバイダ2は、図9について上述したようにコンテンツを自ら作成したコンテンツ鍵で暗号化する。また、コンテンツプロバイダ2は、電子配信サービスセンタ1からコンテンツプロバイダ固有の個別鍵と、配送鍵で暗号化された個別鍵を受け取り、個別鍵によってコンテンツ鍵を暗号化する。かくしてコンテンツプロバイダ2は、コンテンツ鍵で暗号化されたコンテンツと、個別鍵で暗号化されたコンテンツ鍵と、配送鍵で暗号化された個別鍵とをサービスプロバイダ3を介してユーザホームネットワーク5に供給する。

ユーザホームネットワーク5では、電子配信サービスセンタ1から受け取った配送鍵を用いてコンテンツプロバイダ固有の個別鍵を復号化する。これにより、ユーザホームネットワーク5はコンテンツプロバイダ2からコンテンツプロバイダ固有の個別鍵で暗号化されて供給されるコンテンツ鍵を復号することができる。コンテンツ鍵を得たユーザホームネットワーク5は当該コンテンツ鍵によりコンテンツを復号することができる。

ここで、個別鍵はコンテンツサーバごとに固有であるのに対して、配送鍵は一種類のみである。従って、ユーザホームネットワーク5は一種類の配送鍵だけを持っていれば、各コンテンツプロバイダからの個別鍵を復号することができる。

従って、ユーザホームネットワーク 5 は各コンテンツプロバイダ固有の個別鍵を持つ必要がなくなり、配送鍵を持つだけですべてのコンテンツプロバイダのコンテンツを購入することができる。

また、各コンテンツプロバイダは、配送鍵を持たないことにより、他のコンテンツプロバイダ固有の個別鍵（配送鍵で暗号化されている）を復号することができない。これによりコンテンツプロバイダ間でのコンテンツの盗用を防止し得る。

ここで、以上の実施の形態の構成と、特許請求の範囲に記載の発明の各手段とを明らかにするために、各手段の後の括弧内に、対応する実施の形態（但し一例）を付加して本発明の特徴を記述すると、次のようになる。但し勿論この記載は、各手段を記載したものに限定することを意味するものではない。

すなわち、本発明の情報送信システムにおいては、コンテンツ等の情報を送信するコンテンツ供給者又はコンテンツ販売業者（例えば、図 8 4 のコンテンツ送信装置 2 0 0）が持つ個別鍵保存用メモリ（例えば、図 8 4 の耐タンパメモリ 2 0 1）、コンテンツ鍵  $K_c$  を個別鍵  $K_i$  で暗号化するための手段（例えば、図 8 4 のデータ暗号部 2 0 3）、コンテンツ鍵  $K_c$  の使用条件等を記述した取扱方針を生成するための手段（例えば、図 8 4 の取扱方針生成部 2 0 6）、各種データに対してデジタル署名を生成するための手段（例えば、図 8 4 の署名生成部 2 0 7）と、コンテンツを購入するユーザ（例えば、図 8 4 のコンテンツ受信装置 2 1 0）が持つ各種データに対して生成された署名データを検証する手段（例えば、図 8 4 の署名検証部 2 2 2）、コンテンツ鍵  $K_c$  の生成者を示す ID と取扱方針の生成者の ID とを比較するための手段（例えば、図 8 4 の比較器 2 2 6）、配送鍵を保存するための手段（例えば、図 8 4 の耐タンパメモリ 2 2 1）とを備える。

また、本発明の情報送信システムにおいては、コンテンツ等の情報を送信するコンテンツ供給者又はコンテンツ販売業者（例えば、図 8 5 のコンテンツ送信装置 2 0 0）が持つ個別鍵保存用メモリ（例えば、図 8 5 の耐タンパメモリ 2 0 1）、鍵証明書を保存するためのメモリ（例えば、図 8 5 のメモリ 2 0 2）、コンテ

ンツ鍵 $K_c$ を個別鍵 $K_i$ で暗号化するための手段（例えば、図 8 5 のデータ暗号部 2 0 3）、コンテンツを購入するユーザ（例えば、図 8 5 のコンテンツ受信装置 2 1 0）が持つ各種データに対して生成された署名データを検証する手段（例えば、図 8 5 の署名検証部 2 2 2）、配送鍵を保存するための手段（例えば、図 8 5 の耐タンパメモリ 2 2 1）とを備える。

### （3）遠隔再生処理

コンテンツの再生権利を保持していない機器（例えば据置機器 5 2）でコンテンツを保持している機器（例えばホームサーバ 5 1）から再生コマンドを受け取り、コンテンツを再生する遠隔再生処理について説明する。

図 8 6 は遠隔再生処理手順を示し、まず、ユーザの入力操作によって遠隔再生しようとするコンテンツのコンテンツ ID が上位コントローラ 6 2 に入力された後、ステップ S 4 0 1 において、ホームサーバ 5 1 と据置機器 5 2 は相互認証する。相互認証処理は、図 5 2 で説明した処理と同様であるため、説明を省略する。ステップ S 4 0 2 において、ホームサーバ 5 1 の上位コントローラ 6 2 は、ホームサーバ 5 1 の大容量記憶部 6 8 から読み出した登録情報を、ホームサーバ 5 1 の暗号処理部 6 5 に検査させる。上位コントローラ 6 2 から登録情報を受信した暗号処理部 6 5 は、暗号／復号化モジュール 9 6 の署名検証ユニット 1 1 5 に、登録情報に付加されている署名を、暗号処理部 6 5 の記憶モジュール 9 2 から供給された認証局 2 2 の公開鍵で検証させる。署名の検証に成功した後、「登録」の項目が「登録可」になっているか判定し、「登録可」になっていると判定された場合にはステップ S 4 0 3 に進む。なお、据置機器 5 2 側でも登録情報を検査し、ホームサーバ 5 1 が「登録可」になっていることを判定している。

ステップ S 4 0 3 において上位コントローラ 6 2 は遠隔再生しようとするコンテンツのコンテンツ ID を含む再生コマンドを生成し、続くステップ S 4 0 4 において、ホームサーバ 5 1 の暗号処理部 6 5 は、暗号処理部 6 5 の外部メモリ制御部 9 7 に、遠隔再生しようとするコンテンツに対応する使用許諾条件情報及び保存鍵 $K_{save}$ で暗号化されたコンテンツ鍵 $K_c$ を、外部メモリ 6 7 から読み出させ



る。外部メモリ制御部 97 による外部メモリ 67 からのデータ読み出し方法については、図 68 で説明した通りであり、その詳細は省略する。読み出しに成功した場合、ステップ S 405 に進む。

ステップ S 405 において、暗号／復号化モジュール 96 の復号化ユニット 111 は、外部メモリ 67 から読み出したコンテンツ鍵  $K_{co}$  を、記憶モジュール 92 から供給された保存鍵  $K_{save}$  で復号化する。ステップ S 406 において、暗号／復号化モジュール 96 の暗号化ユニット 112 は、一時鍵  $K_{temp}$  でコンテンツ鍵  $K_{co}$  を暗号化した後、ステップ S 407 において再生コマンドを一時鍵  $K_{temp}$  で暗号化する。

ホームサーバ 51 は続くステップ S 408 において、遠隔再生しようとするコンテンツ（コンテンツ鍵  $K_{co}$  で暗号化されている）を大容量記憶部 68 から読み出して、これを上述のステップ S 406 及び S 407 において一時鍵  $K_{temp}$  で暗号化されたコンテンツ鍵及び再生コマンドと共に据置機器 52 に送信する。

ステップ S 409 において、据置機器 52 はホームサーバ 51 から受け取ったコンテンツ鍵及び再生コマンドを一時鍵  $K_{temp}$  で復号化し、ステップ S 410 において暗号処理部 73 と伸張部 74 は相互認証を行い、一時鍵  $K_{temp2}$  を共有する。そしてステップ S 411 において暗号処理部 73 は上述のステップ S 410 において伸張部 74 と共有した一時鍵  $K_{temp2}$  でコンテンツ鍵  $K_{co}$  及び再生コマンドを暗号化する。ステップ S 412 において、暗号処理部 73 は一時鍵  $K_{temp2}$  で暗号化されたコンテンツ鍵  $K_{co}$  及び再生コマンドを伸張部 74 に送信し、伸張部 74 はステップ S 413 においてコンテンツ鍵  $K_{co}$  及び再生コマンドを一時鍵  $K_{temp2}$  で復号化する。

伸張部 74 はステップ S 414 において、ホームサーバ 51 から上述のステップ S 408 においてホームサーバ 51 から受け取ったコンテンツを上述のステップ S 413 において復号化された再生コマンドに従って上述のステップ S 413 において復号化されたコンテンツ鍵  $K_{co}$  で復号化する。そして伸張部 74 は当該復号化されたコンテンツをステップ S 415 において所定の方式、例えば ATR

ACなどの方式により伸張する。ステップS 4 1 6において、上位コントローラ 7 2は暗号処理部 7 3から指示されたデータを電子透かしの形でコンテンツに挿入する。因みに、暗号処理部 7 3から伸張部 7 4へ渡されるデータは、コンテンツ鍵 $K_c$ 、及び再生コマンドだけではなく、再生条件（アナログ出力、デジタル出力、コピー制御信号付き出力（SCMS））、コンテンツ利用権を購入した機器IDなども含まれている。挿入するデータは、このコンテンツ利用権を購入した機器のID、つまりは、使用許諾条件情報内の機器IDなどである。ステップS 4 1 7において、伸張部 7 4は、図示せぬスピーカを介して音楽を再生する。

以上の構成において、ホームサーバ5 1はコンテンツと当該コンテンツの再生コマンド及びコンテンツ鍵 $K_c$ を据置機器5 2に送信することにより、コンテンツの再生権利を保持していない据置機器5 2は、再生コマンド及びコンテンツ鍵 $K_c$ を用いてコンテンツを再生することができる。従って、以上の構成によれば、コンテンツを保持する機器（コンテンツの再生権利を有する機器）に接続された複数の機器（据置機器等）において、コンテンツを再生することができる。

#### （4）予約購入処理

配送鍵の有効期限が切れる前にコンテンツの鍵変換を予め行っておき、コンテンツの購入予約を行うホームサーバの予約購入処理について説明する。図8 7に示す予約購入処理手順のステップS 4 5 1において、ホームサーバ5 1は登録情報更新判断処理を行い、ステップS 4 5 2に進む。登録情報更新判断処理については、図6 1及び図6 2で説明した通りであり、その詳細説明は省略する。但し、予約購入処理においては、図6 1のステップS 6 0 1やS 6 0 2で述べた購入個数や購入金額に基づく登録情報更新タイミングの判断は行わなくても良い。

ステップS 4 5 2において、ホームサーバ5 1の上位コントローラ6 2は、ホームサーバ5 1の大容量記憶部6 8から読み出した登録情報をホームサーバ5 1の暗号処理部6 5に入力する。登録情報を受信した暗号処理部6 5は、暗号／復号化モジュール9 6の署名検証ユニット1 1 5で登録情報の署名を検証した後、ホームサーバ5 1のIDに対する「購入処理」及び「登録」の項目が「購入可」

及び「登録可」になっているか否かを判定し、「購入可」及び「登録可」であった場合にはステップS 4 5 3に進む。ステップS 4 5 3において、ホームサーバ5 1の上位コントローラ6 2は、ホームサーバ5 1の大容量記憶部6 8から読み出したコンテンツプロバイダ2の公開鍵証明書をホームサーバ5 1の暗号処理部6 5に入力する。コンテンツプロバイダ2の公開鍵証明書を受信した暗号処理部6 5は、暗号／復号化モジュール9 6の署名検証ユニット1 1 5でコンテンツプロバイダ2の公開鍵証明書の署名を検証した後、公開鍵証明書からコンテンツプロバイダ2の公開鍵を取り出す。署名の検証の結果、改ざんがなされていないことが確認された場合には、上位コントローラ6 2はステップS 4 5 4に進む。

ステップS 4 5 4においてホームサーバ5 1の上位コントローラ6 2は、ホームサーバ5 1の大容量記憶部6 8から読み出したコンテンツ鍵 $K_c$ をホームサーバ5 1の暗号処理部6 5に入力する。コンテンツ鍵 $K_c$ を受信した暗号処理部6 5は、暗号／復号化モジュール9 6の署名検証ユニット1 1 5でコンテンツ鍵 $K_c$ の署名を検証し、改ざんがなされていないことが確認された場合には、ステップS 4 5 5に進む。

ステップS 4 5 5において、ホームサーバ5 1の上位コントローラ6 2は、ホームサーバ5 1の大容量記憶部6 8から読み出した個別鍵 $K_i$ をホームサーバ5 1の暗号処理部6 5に入力する。個別鍵 $K_i$ を受信した暗号処理部6 5は、暗号／復号化モジュール9 6の署名検証ユニット1 1 5で個別鍵 $K_i$ の署名を検証し、改ざんがなされていないことが確認された場合には、ステップS 4 5 6に進む。

ここで、個別鍵 $K_i$ で暗号化されたコンテンツ鍵 $K_c$ 及び配送鍵 $K_d$ で暗号化された個別鍵 $K_i$ 全体に対して1つの署名がついている場合は、S 4 5 4及びS 4 5 5を1つに合わせることができ署名検証処理を簡略化できる。

ステップS 4 5 6において、暗号処理部6 5の制御部9 1は、ステップS 4 5 5で入力された個別鍵 $K_i$ を、暗号／復号化モジュール9 6の復号化ユニット1 1 1で、記憶モジュール9 2から供給された配送鍵 $K_d$ を用いて復号化する。次

に、暗号処理部 6 5 の制御部 9 1 は、ステップ S 4 5 4 で入力されたコンテンツ鍵  $K_{co}$  を、暗号／復号化モジュール 9 6 の復号化ユニット 1 1 1 で、先ほど復号化した個別鍵  $K_i$  を用いて復号化する。最後に、暗号処理部 6 5 の制御部 9 1 は、暗号／復号化モジュール 9 6 の暗号化ユニット 1 1 2 で、記憶モジュール 9 2 から供給された保存鍵  $K_{save}$  を用いてコンテンツ鍵  $K_{co}$  を暗号化する。

ステップ S 4 5 7 において、保存鍵  $K_{save}$  で暗号化されたコンテンツ鍵  $K_{co}$  は、暗号処理部 6 5 の外部メモリ制御部 9 7 を経由して外部メモリ 6 7 に保存される。

また、ステップ S 4 5 2 でホームサーバ 5 1 が購入処理できない機器であると判定された場合、又はステップ S 4 5 3 でコンテンツプロバイダ 2 の公開鍵証明書の署名が正しくないと判定された場合、又はステップ S 4 5 4 で個別鍵  $K_i$  で暗号化されたコンテンツ鍵  $K_{co}$  の署名が正しくないと判定された場合、又はステップ S 4 5 5 で配送鍵  $K_d$  で暗号化された個別鍵  $K_i$  の署名が正しくないと判定された場合、ホームサーバ 5 1 はステップ S 4 5 8 に進み、エラー処理を行う。

以上のように、ホームサーバ 5 1 は、コンテンツ鍵  $K_{co}$  を個別鍵  $K_i$  で復号化した後、コンテンツ鍵  $K_{co}$  を保存鍵  $K_{save}$  で再暗号化し、外部メモリ 6 7 に記憶させる。この予約購入処理は、実際にコンテンツを購入しないので、図 6 7 について上述した購入処理のうち、ステップ S 1 6 1 の登録情報更新判断処理のなかの課金情報についての処理、ステップ S 1 6 4 に対応する購入コンテンツについての処理、ステップ S 1 6 7 に対応する取扱い方針についての処理、ステップ S 1 6 8 に対応するサービスプロバイダの公開鍵検証についての処理、ステップ S 1 6 9 に対応する価格情報の署名検証についての処理、ステップ S 1 7 0 乃至ステップ S 1 7 2 に対応する課金情報及び使用許諾条件情報の保存処理は行わなくても良い。

因みに、図 8 7 の予約購入処理の場合、ホームサーバ 5 1 は使用許諾条件情報の作成は行わなかったが、これに代えて使用許諾条件情報を作成しその利用権内容番号（すなわち権利項目）を初期値等の権利を持っていない状態（例えば、存

在しない#0など)としておくようにしても良い。

このようにして、予約購入処理では、ホームサーバ51は配送鍵 $K_d$ の有効期限が切れる前にコンテンツ鍵 $K_c$ を外部メモリ67に保存しておくことにより、当該保存されたコンテンツ鍵 $K_c$ によって暗号化されたコンテンツについて、配送鍵 $K_d$ の期限に関わらず購入することができる。

ここで、ホームサーバ51において外部メモリ67にコンテンツ鍵 $K_c$ を保存することにより購入の予約がなされたコンテンツの本購入処理について説明する。図88に示す本購入処理手順のステップS471において、ホームサーバ51は登録情報更新判断処理を行い、ステップS472に進む。登録情報更新判断処理については、図61及び図62で説明した通り、その詳細は、省略する。但し、本購入処理においては、図61のステップS603で述べた配送鍵 $K_d$ に基づく登録情報更新タイミングの判断は行わなくて良い。

ステップS472において、ホームサーバ51の上位コントローラ62は、ホームサーバ51の大容量記憶部68から読み出した登録情報をホームサーバ51の暗号処理部65に入力する。登録情報を受信した暗号処理部65は、暗号/復号化モジュール96の署名検証ユニット115で登録情報の署名を検証した後、ホームサーバ51のIDに対する「購入処理」及び「登録」の項目が「購入可」及び「登録可」になっているか判定し、「購入可」及び「登録可」であった場合にはステップS473に進む。ステップS473において、ホームサーバ51の上位コントローラ62は、ホームサーバ51の大容量記憶部68から読み出したコンテンツプロバイダ2の公開鍵証明書をホームサーバ51の暗号処理部65に入力する。コンテンツプロバイダ2の公開鍵証明書を受信した暗号処理部65は、暗号/復号化モジュール96の署名検証ユニット115でコンテンツプロバイダ2の公開鍵証明書の署名を検証した後、公開鍵証明書からコンテンツプロバイダ2の公開鍵を取り出す。署名の検証の結果、改ざんがなされていないことが確認された場合には、ステップS474に進む。

ステップS474において、ホームサーバ51の上位コントローラ62は、ホ

ームサーバ51の大容量記憶部68から読み出したコンテンツをホームサーバ51の暗号処理部65に入力する。コンテンツを受信した暗号処理部65は、暗号／復号化モジュール96の署名検証ユニット115でコンテンツの署名を検証し、改ざんがなされていないことが確認された場合には、ステップS475に進む。

ステップS475において、ホームサーバ51の上位コントローラ62は、ホームサーバ51の大容量記憶部68から読み出した取扱方針をホームサーバ51の暗号処理部65に入力する。取扱方針を受信した暗号処理部65は、暗号／復号化モジュール96の署名検証ユニット115で取扱方針の署名を検証し、改ざんがなされていないことが確認された場合には、ステップS476に進む。ステップS476において、ホームサーバ51の上位コントローラ62は、ホームサーバ51の大容量記憶部68から読み出したサービスプロバイダ3の公開鍵証明書をホームサーバ51の暗号処理部65に入力する。サービスプロバイダ3の公開鍵証明書を受信した暗号処理部65は、暗号／復号化モジュール96の署名検証ユニット115でサービスプロバイダ3の公開鍵証明書の署名を検証した後、公開鍵証明書からサービスプロバイダ3の公開鍵を取り出す。署名の検証の結果、改ざんがなされていないことが確認された場合には、ステップS477に進む。

ステップS477において、ホームサーバ51の上位コントローラ62は、ホームサーバ51の大容量記憶部68から読み出した価格情報をホームサーバ51の暗号処理部65に入力する。価格情報を受信した暗号処理部65は、暗号／復号化モジュール96の署名検証ユニット115で価格情報の署名を検証し、改ざんがなされていないことが確認された場合には、ステップS478に進む。

ステップS478において、ホームサーバ51の上位コントローラ62は、表示手段64を用いて購入可能なコンテンツの情報（例えば、購入可能な利用形態や価格など）を表示し、ユーザは入力手段63を用いて購入項目を選択する。なお、購入項目の選択処理は本購入処理に先立って行うようにしても良い。入力手

段 6 3 から入力された信号はホームサーバ 5 1 の上位コントローラ 6 2 に送信され、上位コントローラ 6 2 は、その信号に基づいて購入コマンドを生成し、購入コマンドをホームサーバ 5 1 の暗号処理部 6 5 に入力する。これを受信した暗号処理部 6 5 は、ステップ S 4 7 5 で入力された取扱方針及びステップ S 4 7 7 で入力された価格情報から課金情報及び使用許諾条件情報を生成する。課金情報については、図 4 2 で説明した通りであり、その詳細は省略する。また、使用許諾条件情報については、図 4 1 で説明した通りであり、その詳細は省略する。

ステップ S 4 7 9 において、暗号処理部 6 5 の制御部 9 1 は、ステップ S 4 7 8 で生成した課金情報を記憶モジュール 9 2 に保存する。そしてステップ S 4 8 0 において、暗号処理部 6 5 の制御部 9 1 は、ステップ S 4 7 8 で生成した使用許諾条件情報を暗号処理部 6 5 の外部メモリ制御部 9 7 に送信する。使用許諾条件情報を受信した外部メモリ制御部 9 7 は、外部メモリ 6 7 の改ざんチェックを行った後、使用許諾条件情報を外部メモリ 6 7 に書き込む。書き込む際の改ざんチェックについては、図 6 9 について上述した通りであり、詳細説明は省略する（なお、権利なしの使用許諾条件情報がすでに書き込まれている場合には、図 7 0 で説明した書き換え処理により使用許諾条件情報を書き換え更新する）。

因みに、ステップ S 4 7 2 でホームサーバ 5 1 が購入処理できない機器であったり、登録されていないと判定された場合、又はステップ S 4 7 3 でコンテンツプロバイダ 2 の公開鍵証明書の署名が正しくないと判定された場合、又はステップ S 4 7 4 でコンテンツ鍵  $K_c$  で暗号化されたコンテンツの署名が正しくないと判定された場合、又はステップ S 4 7 5 で取扱方針の署名が正しくないと判定された場合、又はステップ S 4 7 6 でサービスプロバイダ 3 の公開鍵証明書の署名が正しくないと判定された場合、又はステップ S 4 7 7 で価格情報の署名が正しくないと判定された場合、ホームサーバ 5 1 はステップ S 4 8 1 に進み、エラー処理を行う。

以上のように、ホームサーバ 5 1 ではユーザが購入選択したコンテンツについての課金情報を記憶モジュール 9 2 に記憶すると共に、使用許諾条件情報を外部

メモリ 67 に記憶することにより、コンテンツの本購入処理を終了する。この本購入処理では、図 87 について上述した予約購入処理で既に行われたコンテンツ鍵  $K_{co}$  の署名検証 (ステップ S 454) 及び個別鍵  $K_i$  の署名検証 (ステップ S 455)、並びにコンテンツ鍵  $K_{co}$  のかけ替え処理 (ステップ S 456) は行わない。

以上の構成において、ホームサーバ 51 では配送鍵  $K_d$  が更新される前に予約購入処理によりコンテンツ鍵  $K_{co}$  を外部メモリ 67 に保存しておくことにより、コンテンツ鍵  $K_{co}$  を復号化する際に必要となる配送鍵  $K_d$  が更新されても、コンテンツ鍵  $K_{co}$  は既に外部メモリ 67 に保存されているので、配送鍵  $K_d$  の有効期限が切れてもコンテンツを購入することができる。

#### (5) 代理購入処理

登録情報 (Registration List) が異なっている機器、すなわちグループが異なっている機器間においてコンテンツの授受を行う代理購入処理について説明する。この代理購入処理では、例えばホームサーバ 51 と当該ホームサーバ 51 に対してグループ外機器である携帯機器等との間でコンテンツを授受する場合について、ホームサーバ 51 側で課金する場合と、グループ外機器で課金を行う場合をそれぞれ説明する。この場合、図 15 について上述した据置機器 52 をグループ外機器として説明する。

図 89 はホームサーバ 51 がグループ外機器にコンテンツを渡し、ホームサーバ 51 が課金処理を行う場合の処理手順を示し、ステップ S 501 において、ホームサーバ 51 とグループ外機器は、相互認証する。相互認証処理は、図 52 で説明した処理と同様であるため、説明を省略する。ステップ S 502 において、ホームサーバ 51 とグループ外機器とは互いに登録情報を交換し、続くステップ S 503 において互いに相手の登録情報を検査する。

すなわち、ホームサーバ 51 はグループ外機器から受け取った登録情報を、暗号処理部 65 に検査させる。グループ外機器からの登録情報を受信した暗号処理部 65 は、暗号/復号化モジュール 96 の署名検証ユニット 115 に、登録情報



に付加されている署名を、暗号処理部 65 の記憶モジュール 92 から供給された公開鍵で検証させる。署名の検証に成功した後、暗号処理部 65 の制御部 91 は、登録情報にグループ外機器の ID が登録され、「購入処理」及び「登録」の項目が「購入可」及び「登録可」になっているか否かを判定する。また、ホームサーバ 51 の登録情報を受け取ったグループ外機器も、同様にしてホームサーバ 51 の登録情報にホームサーバ 51 の ID が登録され、「登録」の項目が「登録可」になっているか否かを判定する。そして、互いに相手の機器が登録されていることが確認されると、ホームサーバ 51 はステップ S 504 に移る。

ステップ S 504 からステップ S 510 は、図 67 のステップ S 161 からステップ S 171 までと同様な処理のため、その詳細は省略する。

ステップ S 511 において、暗号処理部 65 の制御部 91 は、ステップ S 508 で入力された配送鍵  $K_d$  で暗号化された個別鍵  $K_i$  を、暗号／復号化モジュール 96 の復号化ユニット 111 で、記憶モジュール 92 から供給された配送鍵  $K_d$  を用いて復号化する。次に、暗号処理部 65 の制御部 91 は、ステップ S 508 で入力された個別鍵  $K_i$  で暗号化されたコンテンツ鍵  $K_c$  を、暗号／復号化モジュール 96 の復号化ユニット 111 で、先ほど復号化した個別鍵  $K_i$  を用いて復号化する。そして、暗号処理部 65 の制御部 91 は、暗号／復号化モジュール 96 の暗号化ユニット 112 で、ステップ S 501 の相互認証時にグループ外機器と共有した一時鍵  $K_{temp}$  を用いてコンテンツ鍵  $K_c$  を再暗号化する。ステップ S 512 において、暗号処理部 65 の制御部 91 は、一時鍵  $K_{temp}$  で暗号化されたコンテンツ鍵  $K_c$  と、ステップ S 509 で生成した使用許諾条件情報に対し、暗号／復号化モジュール 96 の署名生成ユニット 114 を用いて署名を生成し、上位コントローラ 62 に送信する。一時鍵  $K_{temp}$  で暗号化されたコンテンツ鍵  $K_c$ 、使用許諾条件情報およびそれらの署名を受信したホームサーバ 51 の上位コントローラ 62 は、大容量記憶部 68 からコンテンツ鍵  $K_c$  で暗号化されたコンテンツを読み出し、一時鍵  $K_{temp}$  で暗号化されたコンテンツ鍵  $K_c$ 、使用許諾条件情報、それらの署名およびコンテンツ鍵  $K_c$  で暗号化されたコンテンツをグループ外機器

に送信する。

ステップS 5 1 3において、一時鍵 $K_{temp}$ で暗号化されたコンテンツ鍵 $K_{co}$ 、使用許諾条件情報、それらの署名およびコンテンツ鍵 $K_{co}$ で暗号化されたコンテンツを受信したグループ外機器は、コンテンツ鍵 $K_{co}$ で暗号化されたコンテンツをグループ外機器の記録再生部7 6に出力する。コンテンツ鍵 $K_{co}$ で暗号化されたコンテンツを受信したグループ外機器の記録再生部7 6は、コンテンツ鍵 $K_{co}$ で暗号化されたコンテンツを記録メディア8 0に保存する。

ステップS 5 1 4において、グループ外機器の暗号処理部7 3は、上述のステップS 5 1 2でホームサーバから受け取った署名の検証を行うと共に、一時鍵 $K_{temp}$ で暗号化されたコンテンツ鍵 $K_{co}$ を、暗号／復号化モジュールの復号化ユニットで、ステップS 5 0 1の相互認証時にホームサーバ5 1と共有した一時鍵 $K_{temp}$ を用いて復号化する。そして、暗号処理部7 3の制御部は、暗号／復号化モジュールの暗号化ユニットで、暗号処理部7 3の記憶モジュールから供給された保存鍵 $K_{save2}$ を用いてコンテンツ鍵 $K_{co}$ を再暗号化する。

ステップS 5 1 5において、グループ外機器の暗号処理部7 3は、保存鍵 $K_{save2}$ で暗号化されたコンテンツ鍵 $K_{co}$ とステップS 5 1 3で受信した使用許諾条件情報を暗号処理部7 3の外部メモリ制御部に送信し、外部メモリ7 9に保存させる。外部メモリ制御部が外部メモリにデータを書き込む処理については、図6 9で説明しているので、詳細は省略する。

このように、ホームサーバ5 1はコンテンツ利用権を購入し、課金情報はホームサーバ5 1側で保存し、利用権はグループ外機器に引き渡される。これにより、ホームサーバ5 1はグループ外機器に引き渡したコンテンツ利用権についてその支払いを行うことになる。

次に、図9 0はホームサーバ5 1がグループ外機器にコンテンツを渡し、グループ外機器が課金処理を行う場合の処理手順を示し、ステップS 5 5 1においてグループ外機器は、暗号処理部7 3（図1 5）内に記憶されている課金情報の課金の合計が、上限に達しているか否か判定し、上限に達していなかった場合には

ステップS 5 5 2に進む（なお、課金合計上限で判定するのではなく、課金処理件数の上限で判定するようにしても良い）。

ステップS 5 5 2において、グループ外機器の上位コントローラ 7 2は、外部メモリ 7 9から読み出した登録情報を暗号処理部 7 3に入力する。登録情報を受信した暗号処理部 7 3は、その内部に設けられた暗号／復号化モジュールの署名検証ユニットで登録情報の署名を検証した後、グループ外機器（据置機器 5 2）のIDに対する「購入処理」の項目が「購入可」になっているか判定し、「購入可」であった場合にはステップS 5 5 3に進む。

ステップS 5 5 3において、ホームサーバ 5 1とグループ外機器は、相互認証する。相互認証処理は、図 5 2で説明した処理と同様であるため、説明を省略する。ステップS 5 5 4において、ホームサーバ 5 1とグループ外機器とは互いに登録情報を交換し、続くステップS 5 5 5において互いに相手の登録情報を検査する。

すなわち、ホームサーバ 5 1はグループ外機器から受け取った登録情報を、暗号処理部 6 5に検査させる。グループ外機器からの登録情報を受信した暗号処理部 6 5は、暗号／復号化モジュール 9 6の署名検証ユニット 1 1 5に、登録情報に付加されている署名を、暗号処理部 6 5の記憶モジュール 9 2から供給された公開鍵で検証させる。署名の検証に成功した後、暗号処理部 6 5の制御部 9 1は、登録情報にグループ外機器のIDが登録され、「登録」の項目が「登録可」になっているか否かを判定する。また、ホームサーバ 5 1の登録情報を受け取ったグループ外機器も、同様にしてホームサーバ 5 1の登録情報にホームサーバ 5 1のIDが登録され、「登録」の項目が「登録可」になっているか否かを判定する。なお、同様の処理をグループ外機器も行っている。そして、互いに相手の機器が登録されていることが確認されると、ホームサーバ 5 1はステップS 5 5 6に移る。

ステップS 5 5 6において、ホームサーバ 5 1の制御部 9 1は、外部メモリ制御部 9 7を介して外部メモリ 6 7から既に購入済のコンテンツ鍵を読み出し、続

くステップS 5 5 7においてコンテンツ鍵 $K_c$ を保存鍵 $K_{save}$ で復号化すると共に一時鍵 $K_{temp}$ で再暗号化し、それらの署名を生成する。

ステップS 5 5 8において、ホームサーバ5 1は、S 5 5 7で生成した保存鍵 $K_{temp}$ で暗号化されたコンテンツ鍵と大容量記憶部6 8から読みだしたコンテンツ、取扱方針、価格情報をグループ外機器に送信する。ステップS 5 5 9においてグループ外機器は、ホームサーバ5 1から受け取ったコンテンツを記録メディア8 0に保存する。

ステップS 5 6 0において、グループ外機器（据置機器5 2）は取扱方針、価格情報等の署名を検証した後、ステップS 5 6 1において、グループ外機器の上位コントローラ7 2は、表示手段7 8を用いて購入可能なコンテンツの情報（例えば、購入可能な利用形態や価格など）を表示し、ユーザは入力手段7 7を用いて購入項目を選択する。なお購入項目の選択処理は代理購入処理に先立って行うようにしても良い。入力手段7 7から入力された信号は上位コントローラ7 2に送信され、上位コントローラ7 2は、その信号に基づいて購入コマンドを生成し、購入コマンドを暗号処理部7 3に入力する。これを受信した暗号処理部7 3は、ステップS 5 6 0で入力された取扱方針および価格情報から課金情報および使用許諾条件情報を生成する。課金情報については、図4 2で説明したので、その詳細は省略する。使用許諾条件情報については、図4 1で説明したので、その詳細は省略する。

ステップS 5 6 2において、暗号処理部7 3は、ステップS 5 6 1で生成した課金情報を暗号処理部7 3内の記憶モジュールに保存する。ステップS 5 6 3において、暗号処理部7 3は、ステップS 5 5 7で暗号化されたコンテンツ鍵について、署名を検証すると共に一時鍵 $K_{temp}$ で復号化し、保存鍵 $K_{save2}$ で再暗号化する。そしてステップS 5 6 4において、保存鍵 $K_{save2}$ で暗号化されたコンテンツ鍵 $K_c$ は、暗号処理部7 3から外部メモリ7 9に保存される。

このように、ホームサーバ5 1は既に購入したコンテンツ利用権をグループ外機器に引き渡し、グループ外機器は課金情報も保存することにより、グループ外

機器はグループ外のホームサーバ51から引き渡されたコンテンツ利用権についてその支払いを行うことになる。

以上の構成において、登録情報(Registration List)が異なっている機器間において、上述のステップS502及びステップS554について上述したように、互いの登録情報を交換することにより、登録された機器であることを確認した後一方の機器が有するコンテンツを他方の機器に引き渡すことができる。従って、以上の構成によれば、グループが異なる機器間においてコンテンツの授受を行うことができる。

なお、上述の実施の形態においては、購入処理の際にコンテンツの署名を検証したが、処理に時間がかかるため省略する場合がある。また、取扱方針又は価格情報に、検証の必要性の有無を記述し、それに従って動作する場合がある。

#### (6) 各種データのデータフォーマット

電子配信サービスセンタ1は、コンテンツプロバイダ2毎の個別鍵 $K_i$ にコンテンツプロバイダ2のIDを付加し、当該個別鍵 $K_i$ とコンテンツプロバイダ2のIDの全体に対して配送鍵 $K_d$ を用いて暗号化し、得られたデータを暗号化された個別鍵 $K_i$ として対応するコンテンツプロバイダ2に配送する。

コンテンツプロバイダ2は、このように電子配信サービスセンタ1から与えられた暗号化された個別鍵 $K_i$ をそのままシングルコンテンツ用の鍵データに格納し、当該鍵データをサービスプロバイダ3を介してユーザホームネットワーク5内の機器に配送する。そして、電子音楽配信システム10においては、鍵データに含まれる暗号化された個別鍵 $K_i$ を復号するための配送鍵 $K_d$ がユーザホームネットワーク5内の機器にのみ保有されており、これにより個別鍵 $K_i$ と共に暗号化されたコンテンツプロバイダ2のIDがコンテンツプロバイダ2からコンテンツを購入するユーザホームネットワーク5内の機器までの間で改竄されることをほぼ確実に防止している。

従って、ユーザホームネットワーク5内の機器は、シングルコンテンツおよびアルバムコンテンツの署名が配送途中で改竄されて不当なコンテンツが供給され

たり、または取扱方針等の署名が配送途中に改竄されても、これらシングルコンテンツおよびアルバムコンテンツ並びに取扱方針などに含まれるコンテンツプロバイダ2のIDと、鍵データに含まれる、個別鍵 $K_1$ と共に暗号化されたコンテンツプロバイダ2のIDとを比較することにより当該シングルコンテンツおよびアルバムコンテンツ並びに取扱方針などが正当なデータであるか否かを容易にかつ確実にチェックし得る。

これにより電子音楽配信システム10においては、例えば、不当なコンテンツが購入処理されたり、または不当な取扱方針に基づいて第3者に不当に利益が分配されるような課金情報を生成することをほぼ確実に防止し得、かくして、コンテンツデータが不当に利用されることを防止し得る。

因みに、かかる電子音楽配信システム10においては、サービスプロバイダ3のIDに対してもコンテンツプロバイダ2のIDと同様に暗号化して配送しても良く、この場合にも、例えば、課金情報に含まれるサービスプロバイダ3のIDを改竄して（すなわち価格情報の署名を改竄して）不当に利益を得ようとしても、これを容易かつ確実に防止し得る。

これに加えて、図91は管理移動権の移動処理による世代管理を示すものである。図33および図34について上述したように取扱方針には再生権を最大で何世代目まで移動し得るかが世代管理情報として格納されている。従って、コンテンツプロバイダ2からサービスプロバイダ3を介してユーザホームネットワーク5内の所定の第1の機器に取扱方針が与えられ、当該第1の機器内の暗号処理部において購入処理が実行されると、当該暗号処理部は、取扱方針に含まれる世代管理情報を検出し、当該世代管理情報が示すコンテンツの再購入可能な最大回数を検出する。

そして、暗号処理部は、検出したコンテンツの再購入可能な最大回数に応じて、取扱方針が付加されたコンテンツの購入処理が可能なときには、この取扱方針に基づいて使用許諾条件情報を作成して、当該使用許諾条件情報に暗号処理部のIDを格納すると共に、再購入可能な最大回数から1回分の回数を減らした回数

(すなわち、コンテンツの再購入可能な残り回数)を世代管理情報として格納する。

また、暗号処理部は、購入したコンテンツが暗号処理部の設けられていないコンテンツプロバイダ 2 から供給されたときには、取扱方針に基づいて課金情報を作成するものの、当該課金情報に供給元の ID としていずれの暗号処理部も示さない予め設定された所定の値を格納する。

次いで、第 1 の機器は、使用許諾条件情報に含まれる世代管理情報により購入処理したコンテンツが再配付可能なときには、必要に応じてこのコンテンツを使用許諾条件情報と共に当該第 1 の機器からユーザホームネットワーク 5 内の他の第 2 の機器に再配付する。第 2 の機器において、内部の暗号処理部は、再配付されたコンテンツに対して購入処理を実行すると、当該コンテンツに付加された使用許諾条件情報を作成し直すようにして、この作成し直した使用許諾条件情報に当該暗号処理部の ID を格納すると共に、第 1 の機器において格納された再購入可能な残り回数から 1 回分の回数を減らした回数(すなわち、コンテンツの新たな再購入可能な残り回数)を世代管理情報として格納する。また、暗号処理部は、購入処理に伴い作成した課金情報に供給元の ID として、第 1 の機器内の暗号処理部の ID を格納する。

そして、第 2 の機器は、この後、使用許諾条件情報に含まれる世代管理情報により購入処理したコンテンツが予め設定された購入処理可能な最大回数分、再購入していると、再配付が不可能であると判断して当該コンテンツの再配付を行わないようにする。

かくして、電子音楽配信システム 10 においては、このように世代管理情報によりコンテンツの再購入可能な最大回数を予め取扱方針において規定し、コンテンツの購入処理毎に使用許諾条件情報において当該コンテンツに対する再購入可能な残り回数を管理することにより不当に再購入することを防止し得る。

また、電子音楽配信システム 10 においては、コンテンツを再購入した更に課金情報により当該コンテンツの供給元の ID を累積して格納することにより、必

要に応じて課金情報の供給元のIDからコンテンツの供給ルートを特定することができ、かくして、不正なコンテンツがシステム内に流入した際には当該不正なコンテンツの供給元を探索して排除し得る。

因みに、電子音楽配信システム10においては、コンテンツの再購入時にはコンテンツプロバイダ2やサービスプロバイダ3に代わりユーザホームネットワーク5内の機器が当該コンテンツを提供することにより、例えば、電子配信サービスセンタ1において、課金情報に含まれる供給元のIDに基づいて、コンテンツの再購入の供給元の当該機器を所有するユーザに対して、コンテンツ購入時に使用し得る割引ポイントを加算するなどのように、当該機器に対して利益を還元することもできる。

以上の構成において、電子音楽配信システム10では、コンテンツプロバイダ2からサービスプロバイダ3を介してユーザホームネットワーク5内の機器にコンテンツを提供する場合、当該コンテンツプロバイダ2において、コンテンツ鍵 $K_c$ で暗号化したコンテンツおよびコンテンツプロバイダ2のIDなどが格納されたシングルコンテンツおよびアルバムコンテンツを生成すると共に、当該コンテンツプロバイダ2のIDが格納されたシングルコンテンツおよびアルバムコンテンツの取扱方針を生成し、また、個別鍵 $K_i$ で暗号化したコンテンツ鍵 $K_c$ および配送鍵 $K_d$ で暗号化した個別鍵 $K_i$ などが格納されたシングルコンテンツ用およびアルバムコンテンツ用の鍵データを生成する。

そして、コンテンツプロバイダ2は、これらシングルコンテンツおよびアルバムコンテンツと、シングルコンテンツおよびアルバムコンテンツの取扱方針と、シングルコンテンツ用およびアルバムコンテンツ用の鍵データとをコンテンツプロバイダセキュアコンテナとして送信する。

ここで、コンテンツプロバイダ2は、このとき、配送鍵 $K_d$ で暗号化した個別鍵 $K_i$ として、電子配信サービスセンタ1から供給されたものを用いるが、当該電子配信サービスセンタ1は、個別鍵 $K_i$ にコンテンツプロバイダ2のIDを付加し、これら全体に対して配送鍵 $K_d$ を用いて暗号化する。そして、この暗号化



に用いた配送鍵 $K_d$ は、電子配信サービスセンタ 1 以外には、ユーザホームネットワーク 5 内の機器のみが保持するようにした。

従って、電子音楽配信システム 10 では、配送鍵 $K_d$ で暗号化した個別鍵 $K_i$ をコンテンツプロバイダ 2 からサービスプロバイダ 3 を介してユーザホームネットワーク 5 内の機器まで改竄されることを防止して提供することができ、かくして当該機器において、この配送鍵 $K_d$ で暗号化した個別鍵 $K_i$ を復号化して得られるコンテンツプロバイダ 2 の ID と、シングルコンテンツおよびアルバムコンテンツ、シングルコンテンツおよびアルバムコンテンツの取扱方針にそれぞれ含まれるコンテンツプロバイダ 2 の ID とを比較することにより当該シングルコンテンツおよびアルバムコンテンツ、シングルコンテンツおよびアルバムコンテンツの取扱方針の署名が改竄されたか否かを容易にかつ確実に検出することができる。

この結果、電子音楽配信システム 10 では、不当なコンテンツをユーザに提供したり、または取扱方針を用いて第 3 者が不当に利益を得るような課金情報が生成されることを防止することができ、かくしてコンテンツが第 3 者に不当に利用されることを防止することができる。

また、電子音楽配信システム 10 では、コンテンツプロバイダ 2 から提供する取扱方針にコンテンツの再購入可能な最大回数を格納すると共に、ユーザホームネットワーク 5 内の機器間でコンテンツを再購入する毎に、当該機器において、使用許諾条件情報にコンテンツに対する再購入可能な残り回数を格納する。

従って、電子音楽配信システム 10 では、ユーザホームネットワーク 5 内の機器が使用許諾条件情報により、コンテンツに対する再購入可能な残り回数を管理することができ、かくしてコンテンツが再購入可能な最大回数よりも多く、不当に再購入されることを防止することができる。

以上の構成によれば、コンテンツプロバイダ 2 から暗号化したコンテンツに当該コンテンツプロバイダ 2 の ID を直接付加（すなわち、シングルコンテンツおよびアルバムコンテンツのデータにコンテンツプロバイダ 2 の ID を格納）し、

または間接的に付加（すなわち、コンテンツプロバイダ 2 の ID を格納した取扱方針を付加）し、当該コンテンツプロバイダ 2 の ID を付加したコンテンツと共に、配送鍵  $K_d$  を用いて個別鍵  $K_i$  と共に暗号化したコンテンツプロバイダ 2 の ID をユーザホームネットワーク 5 内の機器に提供し、当該機器において、暗号化されたコンテンツプロバイダ 2 の ID を復号化し、得られたコンテンツプロバイダ 2 の ID と、コンテンツに付加されたコンテンツプロバイダ 2 の ID とを比較するようにしたことにより、コンテンツを正当に利用し得るか否かを容易にかつ確実に判断することができ、かくしてコンテンツが不当に利用されることを防止し得る電子音楽配信システムを実現することができる。

また、コンテンツプロバイダ 2 から提供する取扱方針にコンテンツの再購入可能な最大回数を格納すると共に、ユーザホームネットワーク 5 内の機器間でコンテンツを再購入する毎に、当該機器において、使用許諾条件情報に当該コンテンツに対する再購入可能な残り回数を格納して当該再購入可能な回数を管理するようにしたことにより、コンテンツが再購入可能な最大回数よりも多く、不当に再購入されることを防止することができる。

#### （7）記録再生装置の構成

電子音楽配信システム 10 においては、ユーザホームネットワーク 5 内の機器として、図 9 2 に示す記録再生装置 250 が設けられている。そして、かかる記録再生装置 250 には、データ格納装置である電子配信専用記録メディア 251 が着脱自在に設けられている。

記録再生装置 250 は、サービスプロバイダ 3 からネットワーク 4 を介して電子配信されたコンテンツを電子配信専用記録メディア 251 に記録し、当該電子配信専用記録メディア 251 からコンテンツを再生し得る。

実際に記録再生装置 250 は、受信手段である通信部 260、記録再生制御手段である上位コントローラ 261、暗号処理部 262、コンテンツ復号手段である伸張部 263、入力手段 264、表示手段 265、および大容量記憶部 266 から構成される。通信部 260 は、電子配信サービスセンタ 1 との間で通信する

と共に、ネットワーク 4 を介してサービスプロバイダ 3 との間で通信する。

上位コントローラ 261 は、購入処理時、入力手段 264 を介して入力された操作命令に基づいて、記録再生装置 250 および電子配信専用記録メディア 251 を制御することにより、通信部 260 によって受信したコンテンツプロバイダセキュアコンテナおよびサービスプロバイダセキュアコンテナを一旦、大容量記憶部 266 に保持する。

そして、上位コントローラ 261 は、電子配信専用記録メディア 251 に購入処理を実行させ、これにより大容量記憶部 266 から対応するコンテンツ鍵  $K_{co}$  で暗号化されているコンテンツ、個別鍵  $K_i$  で暗号化されているコンテンツ鍵  $K_{co}$  および配送鍵  $K_d$  で暗号化されている個別鍵  $K_i$  を読み出し、電子配信専用記録メディア 251 において、配送鍵  $K_d$  で暗号化されている個別鍵  $K_i$  を暗号処理部 301 の記憶モジュール 311 から読み出した配送鍵  $K_d$  で復号化し、個別鍵  $K_i$  で暗号化されているコンテンツ鍵  $K_{co}$  を当該復号化した個別鍵  $K_i$  で復号化し、得られたコンテンツ鍵  $K_{co}$  を暗号処理部 301 の記憶モジュール 311 から読み出した保存鍵  $K_{save}$  で暗号化し、当該読み出したコンテンツ鍵  $K_{co}$  で暗号化されているコンテンツおよび保存鍵  $K_{save}$  で暗号化されているコンテンツ鍵  $K_{co}$  を当該電子配信専用記録メディア 251 に記録する。

また、上位コントローラ 261 は、再生処理時、入力手段 264 を介して入力された操作命令に基づいて、記録再生装置 250 および電子配信専用記録メディア 251 を制御することにより、当該電子配信専用記録メディア 251 から、(相互認証により暗号処理部 262 と暗号処理部 301 との間で共有化した) 一時鍵  $K_{temp1}$  で暗号化されているコンテンツ鍵  $K_{co}$  を読み出し、(相互認証により暗号処理部 262 と伸張部 263 との間で共有化した) 一時鍵  $K_{temp2}$  で暗号化されているコンテンツ鍵  $K_{co}$ 、当該コンテンツ鍵  $K_{co}$  で暗号化されているコンテンツを伸張部 263 に供給して当該コンテンツ鍵  $K_{co}$  で暗号化されているコンテンツをコンテンツ鍵  $K_{co}$  を用いて復号化させる。

因みに、入力手段 264 および表示手段 265 は、それぞれホームサーバ 51

の入力手段 6 3 および表示手段 6 4 と同様の機能を有しているため、その説明は省略する。

暗号処理部 2 6 2 は、制御部 2 7 0、記憶モジュール 2 7 1、登録情報検査モジュール 2 7 2、購入処理モジュール 2 7 3、相互認証モジュール 2 7 4、暗号／復号化モジュール 2 7 5 から構成されている。因みに、この暗号処理部 2 6 2 は、ホームサーバ 5 1 の暗号処理部 6 5 と同様にシングルチップの暗号処理専用 IC で構成され、外部から不正にデータを読み出し難い特性（耐タンパ性）を有する。

そして、暗号処理部 2 6 2 において、制御部 2 7 0、記憶モジュール 2 7 1、登録情報検査モジュール 2 7 2、購入処理モジュール 2 7 3、暗号／復号化モジュール 2 7 5 は、ホームサーバ 5 1 の制御部 9 1、記憶モジュール 9 2、登録情報検査モジュール 9 3、購入処理モジュール 9 4、暗号／復号化モジュール 9 6 と同様の機能を有しているため、その説明は省略する。

また、相互認証モジュール 2 7 4 は、伸張部 2 6 3 や、電子配信専用記録メディア 2 5 1 との間で相互認証を実行し、必要に応じて伸張部 2 6 3 や、電子配信専用記録メディア 2 5 1 と共有化する一時鍵  $K_{temp}$ （セッション鍵）を生成する。

暗号／復号化モジュール 2 7 5 は、復号化ユニット 2 8 0、暗号化ユニット 2 8 1、乱数発生ユニット 2 8 2、署名生成ユニット 2 8 3、および署名検証ユニット 2 8 4 から構成される。復号化ユニット 2 8 0、暗号化ユニット 2 8 1、乱数発生ユニット 2 8 2、署名生成ユニット 2 8 3、および署名検証ユニット 2 8 4 は、それぞれホームサーバ 5 1 の復号化ユニット 1 1 1、暗号化ユニット 1 1 2、乱数発生ユニット 1 1 3、署名生成ユニット 1 1 4、および署名検証ユニット 1 1 5 と同様の機能を有しているため、その説明は省略する。

伸張部 2 6 3 は、相互認証モジュール 2 9 0、鍵復号化モジュール 2 9 1、復号化モジュール 2 9 2、伸張モジュール 2 9 3、電子透かし付加モジュール 2 9 4、および記憶モジュール 2 9 5 から構成される。相互認証モジュール 2 9 0、鍵復号化モジュール 2 9 1、復号化モジュール 2 9 2、伸張モジュール 2 9 3、

電子透かし付加モジュール２９４、および記憶モジュール２９５は、それぞれホームサーバ５１の相互認証モジュール１０１、鍵復号化モジュール１０２、復号化モジュール１０３、伸張モジュール１０４、電子透かし付加モジュール１０５、および記憶モジュール１０６と同様の機能を有しているため、その説明は省略する。

また、電子配信専用記録メディア２５１は、購入処理を実行して課金情報を作成し、当該作成した課金情報を保持するようになされており、通信手段である通信部３００、コンテンツ鍵暗号手段およびコンテンツ鍵復号手段である暗号処理部３０１、記録再生手段である外部メモリ制御部３０２、および記録媒体である外部メモリ３０３から構成される。

通信部３００は記録再生装置２５０の上位コントローラ２６１との間でデータの送受信を行う。暗号処理部３０１は、ホームサーバ５１の暗号処理部６５と同様の回路構成でなり、外部から不正にデータを読み出し難い特性（耐タンパ性）を有する。また、暗号処理部３０１は、制御部３１０、保存鍵保持手段である記憶モジュール３１１、登録情報検査モジュール３１２、購入処理モジュール３１３、相互認証モジュール３１４、および暗号／復号化モジュール３１５から構成される。

制御部３１０、記憶モジュール３１１、登録情報検査モジュール３１２、購入処理モジュール３１３、相互認証モジュール３１４、および暗号／復号化モジュール３１５は、それぞれホームサーバ５１の制御部９１、記憶モジュール９２、登録情報検査モジュール９３、購入処理モジュール９４、相互認証モジュール９５、および暗号／復号化モジュール９６と同様の機能を有しているため、その説明は省略する。因みに、暗号／復号化モジュール３１５は、復号化ユニット３２０、暗号化ユニット３２１、乱数発生ユニット３２２、署名生成ユニット３２３、および署名検証ユニット３２４から構成される。

外部メモリ制御部３０２は、外部メモリ３０３にデータを読み書きする他に、必要に応じて改竄チェック処理を行う。外部メモリ３０３としては、書き込み可

能な光ディスク、ハードディスク、半導体メモリ等のように種々の記録媒体を適用し得る。従って、外部メモリ制御部 302 としては、これらの記録媒体からデータを読み出せる構造が必要であり、必要であれば図示せぬ記録媒体制御部を付加して読み書きを行う。なお、改竄チェック処理の詳細については、図 68 から図 71 で説明したのでその説明は省略する。

ここで、かかる電子配信専用記録メディア 251 においては、暗号処理部 301 の記憶モジュール 311 に当該電子配信専用記録メディア 251 固有の保存鍵  $K_{save}$  を保持している。そして、電子配信専用記録メディア 251 においては、コンテンツ鍵  $K_c$  を外部メモリ 303 に記録する際に、当該コンテンツ鍵  $K_c$  を保存鍵  $K_{save}$  で暗号化し、また、外部メモリ 303 からこの暗号化されているコンテンツ鍵  $K_c$  を再生したときには、当該コンテンツ鍵  $K_c$  を保存鍵  $K_{save}$  で復号化して記録再生装置 250 に送信する。

従って、従来の記録再生装置により記録メディアに記録されたコンテンツは、当該記録メディアにコンテンツを記録した機器（すなわち、記録メディアに記録するコンテンツ鍵  $K_c$  を暗号化した暗号処理部固有の保存鍵  $K_{save}$  を保持する機器）以外の他の機器（すなわち、コンテンツを暗号化した保存鍵  $K_{save}$  とは異なる保存鍵  $K_{save}$  を保持する機器）では再生することができないものの、この電子配信専用記録メディア 251 に記録されたコンテンツは、上述した記録再生装置 250 と同様の構成を有する機器であれば、保存鍵  $K_{save}$  を保持していなくても再生することができる。

ところで、かかる記録再生装置 250 においては、電子配信専用記録メディア 251 において、購入処理を実行してコンテンツをコンテンツ鍵  $K_c$  と共に記録するため、当該コンテンツの記録だけを目的として、暗号処理部 262 および伸張部 263 を用いずに構成することもできる。

また、かかる記録再生装置 250 においては、電子配信専用記録メディア 251 が着脱自在に設けられ、他の機器でコンテンツおよびコンテンツ鍵  $K_c$  を記録した電子配信専用記録メディア 251 からでも当該コンテンツを再生し得るため

、当該記録再生装置 250 に再生機能だけを持たせるようにして、電子配信サービスセンタ 1 やネットワーク 4 に接続せずに用いることもできる。

ところが、ユーザホームネットワーク 5 内においては、電子配信専用記録メディア 251 に対して、このようにネットワーク 4 に接続された記録再生装置 250 において、コンテンツおよびコンテンツ鍵  $K_c$  を記録し、電子配信サービスセンタ 1 やネットワーク 4 に接続されていない記録再生装置 250 で当該コンテンツを再生するために用いられると、当該電子配信専用記録メディア 251 が保持する課金情報を電子配信サービスセンタ 1 において回収し難くなることが考えられる。

このため、電子配信専用記録メディア 251 においては、暗号処理部 301 において、制御部 310 から、例えば、定期的に記憶モジュール 311 内の課金情報を検索し、電子配信サービスセンタ 1 に未回収の課金情報があるときには、対応するコンテンツに対して再生制限を加えて、例えば、購入処理から課金情報が回収されるまでの間にコンテンツを一回しか再生することができないようにすると共に、当該コンテンツの管理移動も行わないようにする。

これにより、電子音楽配信システム 10 では、電子配信専用記録メディア 251 を所有するユーザが不当にコンテンツを再生することを防止する。因みに、課金情報の未回収による再生制限としては、例えば、購入処理から課金情報が回収されるまでの間にコンテンツを再生し得る回数を予め設定し、購入処理した時点からコンテンツの再生回数をカウントし、課金情報が未回収であることを検出した際に、再生制限を有効に機能させることもできる。すなわち、課金情報が未回収であることを検出したとき、この時点における対応するコンテンツの既に再生された回数と、予め設定した再生制限の回数とを比較し、当該コンテンツを既に再生した回数が、設定した再生制限の回数に達しているときには、このコンテンツを再生できないようにする。

また、かかる再生制限としては、期間（時間）を用いるようにしても良い。すなわち、コンテンツを再生し得る時間を予め設定し、購入処理してから当該設定

した時間を経過しても課金情報が未回収の場合にはコンテンツを再生できなくする。なお、電子配信専用記録メディア 251 においては、再生制限の制限内容を、例えば、暗号処理部 301 の記憶モジュール 311 内に課金情報に対応させて保持し、または、外部メモリ 303 に使用許諾条件情報に対応させて保持しても良い。また、再生制限（回数または期間）を取扱方針およびまたは価格情報に格納しておき、電子配信専用記録メディア 251 は、購入処理の際に、取扱方針およびまたは価格情報から再生制限の情報を取り出し、これを含む使用許諾条件情報を作成し、当該作成した使用許諾条件情報を外部メモリ 303 に保持しても良い。

ここで、記録再生装置 250 において実行される購入処理を、図 93 に示すフローチャートを用いて説明する。ステップ S700 において、記録再生装置 250 内の上位コントローラ 261 は、サービスプロバイダ 3 からネットワーク 4 を介して配信されたコンテンツプロバイダセキュアコンテナおよびサービスプロバイダセキュアコンテナを大容量記憶部 266 に一旦保持した状態において、電子配信専用記録メディア 251 内の暗号処理部 301 の制御部 310 を介して当該暗号処理部 301 内の記憶モジュール 311 に記憶されている配送鍵  $K_d$  の有効期限（バージョン）を判定し、当該配送鍵  $K_d$  が有効である場合にはステップ S701 に進む。

ステップ S701 において、上位コントローラ 261 は、電子配信専用記録メディア 251 内の暗号処理部 301 の制御部 310 を介して当該暗号処理部 301 内の記憶モジュール 311 に記憶されている課金情報の課金の合計が予め設定された上限に達しているか否かを判断し、当該課金の合計が上限に達していない場合にはステップ S702 に進む。因みに、このステップ S701 では、課金の合計が上限に達したか否かを判断するのではなく、例えば、記憶モジュール 311 における課金情報の記憶エリアに空きがあるか否かを判断し、当該記憶エリアに空きがある場合にステップ S702 に進むようにしても良い。また、ステップ S701 では、記憶モジュール 311 に記憶されている課金情報の数（つまり、購



入回数)が予め設定された(上限の)数に達しているか否かを判断するようにしても良い。

ステップS702において、上位コントローラ261は、大容量記憶部266内のコンテンツプロバイダセキュアコンテナに含まれるコンテンツプロバイダ2の公開鍵証明書を読み出し、当該読み出したコンテンツプロバイダ2の公開鍵証明書を電子配信専用記録メディア251内の暗号処理部301に送信する。これにより、電子配信専用記録メディア251内の暗号処理部301において、制御部310は、暗号/復号化モジュール315内の署名検証ユニット324において、コンテンツプロバイダ2の公開鍵証明書の署名を検証し、この署名の検証の結果、公開鍵証明書に対して改竄がなされていないことが確認されると、当該公開鍵証明書に含まれるコンテンツプロバイダ2の公開鍵を取り出し、ステップS703に進む。

ステップS703において、上位コントローラ261は、大容量記憶部266内のコンテンツプロバイダのセキュアコンテナに含まれるコンテンツの鍵データを読み出し、当該読み出した鍵データを電子配信専用記録メディア251内の暗号処理部301に送信する。これにより、電子配信専用記録メディア251内の暗号処理部301において、制御部310は、暗号/復号化モジュール315内の署名検証ユニット324において、鍵データの署名を検証し、この署名の検証の結果、鍵データに対して改竄がなされていないことが確認されると、ステップS704に進む。

ステップS704において、上位コントローラ261は、大容量記憶部266内のコンテンツプロバイダセキュアコンテナに含まれるコンテンツの取扱方針を読み出し、当該読み出した取扱方針を電子配信専用記録メディア251内の暗号処理部301に送信する。これにより、電子配信専用記録メディア251内の暗号処理部301において、制御部310は、暗号/復号化モジュール315内の署名検証ユニット324において、取扱方針の署名を検証し、この署名の検証の結果、取扱方針に対して改竄がなされていないことが確認されると、ステップS

705に進む。

ステップS705において、上位コントローラ261は、大容量記憶部266内のサービスプロバイダセキュアコンテナに含まれるサービスプロバイダ3の公開鍵証明書を読み出し、当該読み出したサービスプロバイダ3の公開鍵証明書を電子配信専用記録メディア251内の暗号処理部301に送出する。これにより、電子配信専用記録メディア251内の暗号処理部301において、制御部310は、暗号／復号化モジュール315内の署名検証ユニット324において、サービスプロバイダ3の公開鍵証明書の署名を検証し、この署名の検証の結果、鍵データに対して改竄がなされていないことが確認されると、ステップS706に進む。

ステップS706において、上位コントローラ261は、大容量記憶部266内のサービスプロバイダのセキュアコンテナに含まれるコンテンツの価格情報を読み出し、当該読み出した価格情報を電子配信専用記録メディア251内の暗号処理部301に送信する。これにより、電子配信専用記録メディア251内の暗号処理部301において、制御部310は、暗号／復号化モジュール315内の署名検証ユニット324において、価格情報の署名を検証し、この署名の検証の結果、取扱方針に対して改竄がなされていないことが確認されると、ステップS707に進む。

ステップS707において、上位コントローラ261は、表示手段265に購入可能なコンテンツの情報を表示し、ユーザが入力手段264を介して所望するコンテンツを選択指定すると、当該選択指定されたコンテンツに対する購入コマンドを生成して電子配信専用記録メディア251内の暗号処理部301に送信する。これにより、暗号処理部301の制御部310は、購入処理モジュール313において、取扱方針（ステップS704において署名検証した取扱方針）および価格情報（ステップS706により署名検証した価格情報）に基づいて、課金情報および使用許諾条件情報を生成し、ステップS708に進む。因みに、入力手段264を介してユーザに所望するコンテンツを選択指定させるのは、購入処

理に先立ち予め行うようにしても良い。

ステップS 7 0 8において、電子配信専用記録メディア2 5 1内の暗号処理部3 0 1の制御部3 1 0は、課金情報（ステップS 7 0 7において生成した課金情報）を記憶モジュール3 1 1に保存し、続くステップS 7 0 9において、使用許諾条件情報（ステップS 7 0 7において生成した使用許諾条件情報）を外部メモリ制御部3 0 2を介して外部メモリ3 0 3に送出し、かくして外部メモリ3 0 3に使用許諾条件情報を書き込む。また、使用許諾条件情報は、図6 9について上述したデータの書き込み時と同様に、（図1 6の外部メモリと同様にして）改竄防止領域に書き込むようにしても良い。因みに、使用許諾条件情報は、電子配信専用記録メディア2 5 1内の暗号処理部3 0 1の記憶モジュール3 1 1に保存するようにしても良い。

ステップS 7 1 0において、電子配信専用記録メディア2 5 1内の暗号処理部3 0 1の制御部3 1 0は、暗号／復号化モジュール3 1 5の復号化ユニット3 2 0において、鍵データ（上述したステップS 7 0 3において署名検証した鍵データ）に含まれる暗号化されている個別鍵 $K_i$ を、配送鍵 $K_d$ （上述したステップS 7 0 0において有効であることが確認された配送鍵 $K_d$ ）を用いて復号化する。

次いで、制御部3 1 0は、復号化ユニット3 2 0において、鍵データに含まれる暗号化されているコンテンツ鍵 $K_c$ を、先に復号化した個別鍵 $K_i$ を用いて復号化する。続いて、制御部3 1 0は、この復号化したコンテンツ鍵 $K_c$ と、記憶モジュール3 1 1に記憶されている保存鍵 $K_{save}$ とを暗号化ユニット3 2 1に与え、当該暗号化ユニット3 2 1において、保存鍵 $K_{save}$ を用いてコンテンツ鍵 $K_c$ を暗号化する。

ステップS 7 1 1において、電子配信専用記録メディア2 5 1内の暗号処理部3 0 1の制御部3 1 0は、ステップS 7 1 0において、保存鍵 $K_{save}$ で暗号化したコンテンツ鍵 $K_c$ を外部メモリ制御部3 0 2を介して外部メモリ3 0 3に送出し、これにより当該外部メモリ3 0 3に暗号化したコンテンツ鍵 $K_c$ を保存し、ス

ステップS 7 1 2に進む。また、保存鍵 $K_{save}$ で暗号化したコンテンツ鍵 $K_c$ は、図 6 9 について上述したデータの書き込み時と同様に、（図 1 6 の外部メモリと同様にして）改竄防止領域に書き込むようにしても良い。因みに、保存鍵 $K_{save}$ で暗号化したコンテンツ鍵 $K_c$ は、電子配信専用記録メディア 2 5 1 内の暗号処理部 3 0 1 の記憶モジュール 3 1 1 に保存するようにしても良い。

ステップS 7 1 2において、記録再生装置 2 5 0 内の上位コントローラ 2 6 1 は、大容量記憶部 2 6 6 内のコンテンツプロバイダセキュアコンテナに含まれる暗号化されたコンテンツを読み出し、当該読み出した暗号化されているコンテンツを電子配信専用記録メディア 2 5 1 に送出し、かくして電子配信専用記録メディア 2 5 1 内の外部メモリ 3 0 3 にこの暗号化されているコンテンツを保存する。

因みに、このステップS 7 1 2において、上位コントローラ 2 6 1 は、暗号化されているコンテンツと共に、対応するステップS 7 0 4 において署名検証した取扱方針およびステップS 7 0 6 において署名検証した価格情報も外部メモリ 3 0 3 に保存するようにしても良い。また、暗号化されているコンテンツ（または、コンテンツおよび取扱方針並びに価格情報）は、このステップS 7 1 2 において、外部メモリ 3 0 3 に保存せずに、当該ステップS 7 1 2 よりも以前のステップにおいて外部メモリ 3 0 3 に保存するようにしても良い。

そして、かかる購入処理においては、ステップS 7 0 0 において、配送鍵 $K_d$ の有効期限が切れている場合、ステップS 7 0 1 において、課金情報の課金の合計が上限に達していた場合、ステップS 7 0 2 において、コンテンツプロバイダ 2 の公開鍵証明書が正しくないと判定した場合、ステップS 7 0 3 において、鍵データの署名が正しくないと判定した場合、ステップS 7 0 4 において、取扱方針の署名が正しくないと判定した場合、ステップS 7 0 5 において、サービスプロバイダ 3 の公開鍵証明書が正しくないと判定した場合、ステップS 7 0 6 において、価格情報の署名が正しくないと判定した場合には、それぞれステップS 7 1 3 に進んでエラー処理を実行する。因みに、かかる購入処理においては、コンテ

ンツの署名を検証しない場合を示したが、当該コンテンツの外部メモリ 303 への保存に先立ち、いずれかのステップにおいてこのコンテンツの署名を検証するようにしても良い。

因みに、記録再生装置 250 と、電子配信専用記録メディア 251 との間でデータを送受信する場合には、必要に応じて、送信側において当該データに署名を付加し、受信側でこの署名を検証する。

以上のように、記録再生装置 250 は、電子配信専用記録メディア 251 内において購入処理を実行し、かくして電子配信専用記録メディア 251 の外部メモリ 303 にコンテンツ鍵  $K_c$  で暗号化されているコンテンツ、および当該電子配信専用記録メディア 251 の暗号処理部 301 固有の保存鍵  $K_{sav}$  で暗号化されたコンテンツ鍵  $K_c$  をこの電子配信専用記録メディア 251 内の外部メモリ 303 に記録する。

また、記録再生装置 250 において実行される再生処理を、図 94 に示すフローチャートを用いて説明する。ステップ S720 において、記録再生装置 250 内の上位コントローラ 261 は、ユーザにより入力手段 264 を介して再生指示されたコンテンツの ID を電子配信専用記録メディア 251 内の暗号処理部 301 に送出する。

ステップ S721 において、電子配信専用記録メディア 251 内の暗号処理部 301 の制御部 310 は、上位コントローラ 261 から与えられるコンテンツの ID を外部メモリ制御部 302 に送出することにより、当該外部メモリ制御部 302 を介して外部メモリ 303 から当該 ID に対応する、暗号化されているコンテンツ鍵  $K_c$  および使用許諾条件情報を読み出し、当該読み出した暗号化されているコンテンツ鍵  $K_c$  を暗号／復号化モジュール 315 の復号化ユニット 320 に送出すると共に、当該使用許諾条件情報を制御部 310 に送出する。なお、外部メモリ制御部 302 は、外部メモリ 303 から暗号化されているコンテンツ鍵  $K_c$  および使用許諾条件情報を読み出す際に、図 68 について上述したデータの読み出し時と同様に改竄チェックを行うようにしても良い。因みに、電子配信専

用記録メディア 251 においては、暗号化されているコンテンツ鍵  $K_c$ 。および使用許諾条件情報を暗号処理部 301 の記憶モジュール 311 内に保持しておき、当該記憶モジュール 311 から読み出すようにしても良い。

これに加えて暗号処理部 301 の制御部 310 は、ステップ S 722 において、コンテンツの ID に基づいて、記憶モジュール 311 内の課金情報を検索し、続くステップ S 723 において、当該記憶モジュール 311 内にコンテンツの ID に対応する課金情報があるか否かを判断し、当該 ID に対応する課金情報が電子配信サービスセンタ 1 に既に回収され、記憶モジュール 311 内に存在しない場合には、ステップ S 724 に進む。

ステップ S 724 において、暗号処理部 301 の制御部 310 は、使用許諾条件情報を必要に応じて更新する。すなわち、制御部 310 は、使用許諾条件情報に含まれる利用権内容が例えば回数権の場合、その回数権の示す再生回数を減算することを示す。そして、更新した使用許諾条件情報を外部メモリ制御部 302 を介して外部メモリ 303 に保存する。このとき、外部メモリ制御部 302 は、図 70 について上述したデータの書換え時と同様に、改竄チェックを行うようにしても良い。因みに、使用許諾条件情報を暗号処理部 301 の記憶モジュール 311 において、更新して保存するようにしても良い。

次いで、ステップ S 725 において、電子配信専用記録メディア 251 内の暗号処理部 301 の制御部 310 は、記録再生装置 250 の暗号処理部 262 との間で互いの相互認証モジュール 314 および 274 を用いて相互認証を行い、一時鍵  $K_{temp1}$  を共有化し、ステップ S 726 に進む。因みに、相互認証処理手順については、図 51 について上述したため、その詳細な説明は省略する。

ステップ S 726 において、電子配信専用記録メディア 251 内の暗号処理部 301 の制御部 310 は、復号化ユニット 320 において、暗号化されているコンテンツ鍵  $K_c$ 。を記憶モジュール 311 に記憶されている保存鍵  $K_{save}$  で復号化し、当該復号化したコンテンツ鍵  $K_c$ 。を暗号化ユニット 321 に送出する。次いで、制御部 310 は、暗号化ユニット 321 において、ステップ S 625 において

、相互認証モジュール 274 と共有化した一時鍵  $K_{temp1}$  を用いてコンテンツ鍵  $K_c$  を暗号化し、ステップ S 727 に進む。

ステップ S 727 において、電子配信専用記録メディア 251 内の暗号処理部 301 の制御部 310 は、一時鍵  $K_{temp1}$  で暗号化したコンテンツ鍵  $K_c$  を記録再生装置 250 の暗号処理部 262 に送信する。

ステップ S 728 において、記録再生装置 250 内の暗号処理部 262 の制御部 270 は、電子配信専用記録メディア 251 から送信された、暗号化されているコンテンツ鍵  $K_c$  を暗号／復号化モジュール 275 の復号化ユニット 280 に取り込み、当該復号化ユニット 280 において、暗号化されているコンテンツ鍵  $K_c$  をステップ S 725 において、相互認証モジュール 314 と共有化した一時鍵  $K_{temp1}$  を用いて復号化し、当該復号化したコンテンツ鍵  $K_c$  を暗号化ユニット 281 に送出する。

次いで、ステップ S 729 において、記録再生装置 250 内の暗号処理部 262 の制御部 270 は、伸張部 263 との間で互いの相互認証モジュール 274 および 290 を用いて相互認証を行い、一時鍵  $K_{temp2}$  を共有化する。因みに、相互認証処理手順については、図 51 について上述したため、その詳細な説明は省略する。

これにより記録再生装置 250 内の暗号処理部 262 の制御部 270 は、ステップ S 730 において、暗号化ユニット 281 により、伸張部 263 と共有化した一時鍵  $K_{temp2}$  でコンテンツ鍵  $K_c$  を暗号化し、かくして、続くステップ S 731 において、この暗号化したコンテンツ鍵  $K_c$  を伸張部 263 に送出する。

ステップ S 732 において、伸張部 263 の鍵復号モジュール 291 は、暗号処理部 262 から与えられる暗号化されているコンテンツ鍵  $K_c$  を取り込み、当該暗号化されているコンテンツ鍵  $K_c$  を、暗号処理部 262 と共有化した一時鍵  $K_{temp2}$  を用いて復号化し、当該復号化したコンテンツ鍵  $K_c$  を復号化モジュール 292 に送出する。

ステップ S 733 において、伸張部 263 の復号モジュール 292 は、このと

き上位コントローラ 261 から、電子配信専用記録メディア 251 内の外部メモリ 303 から読み出した暗号化されているコンテンツが与えられ、当該暗号化されているコンテンツを、鍵復号モジュール 291 から与えられるコンテンツ鍵 K<sub>0</sub>を用いて復号化し、当該復号化したコンテンツを伸張モジュール 293 に送出する。

ステップ S 734 において、伸張部 263 の伸張モジュール 293 は、復号モジュール 292 から与えられるコンテンツを ATRAC 等の所定の方式により伸張し、当該伸張したコンテンツを電子透かし付加モジュール 294 に送出する。ステップ S 735 において、伸張部 263 の電子透かし付加モジュール 294 は、伸張モジュール 293 から与えられる伸張されたコンテンツに、暗号処理部 262 の制御部 270 によって指示された、電子配信専用記録メディア 251 の暗号処理部 301 の ID 等の所定のデータを電子透かしの形で挿入する。

そして、ステップ S 736 において、記録再生装置 250 内の上位コントローラ 261 は、伸張部 263 において得られたコンテンツを、例えば、スピーカ（図示せず）に送出することにより当該スピーカを介してコンテンツに基づく音楽を放音させる。かくして、記録再生装置 250 は、このようにしてコンテンツを再生し得る。

ここで、ステップ S 723 において、電子配信専用記録メディア 251 内の暗号処理部 301 の制御部 310 は、記憶モジュール 311 にコンテンツの ID に対応する課金情報が保存されている場合には、ステップ S 737 に進んで、課金情報が未回収のときの再生制限を参照し、当該課金情報が未回収のコンテンツが再生可能条件を満たしているか否かを判断する。

そして、暗号処理部 301 の制御部 310 は、コンテンツが再生可能条件を満たしていなければ（すなわち、当該コンテンツが再生制限に定められた回数だけ既に再生された場合、または再生可能期間を経過した場合）、この再生処理を終了する。これに対して制御部 310 は、コンテンツが再生可能条件を満たしていれば（すなわち、当該コンテンツの再生回数が再生制限に定められた回数に満たな



い場合)、ステップS 7 2 4に進み、使用許諾条件情報を必要に応じて更新する。因みに、課金情報が未回収であるときに使用する再生制限は、電子配信専用記録メディア2 5 1内の暗号処理部3 0 1の記憶モジュール3 1 1や、外部メモリ3 0 3に保持していても良いし、取扱方針や価格情報のデータなどに格納しておいても良い。

因みに、電子配信専用記録メディア2 5 1は、図1 5について上述したホームサーバ5 1や、据置機器5 2に設けるようにしても良い。

以上のように、記録再生装置2 5 0においては、電子配信専用記録メディア2 5 1からコンテンツ鍵 $K_{co}$ で暗号化されているコンテンツおよび当該コンテンツ鍵 $K_{co}$ を再生し、このコンテンツ鍵 $K_{co}$ で暗号化されているコンテンツを当該コンテンツ鍵 $K_{co}$ で復号化し得るものの、課金情報が回収されるまでの間は、予め設定された再生制限に従ってコンテンツを利用し得るようにし、また、課金情報が回収された後には、購入処理によって購入した利用権内容に応じてコンテンツを利用し得るようにする。

以上の構成において、この電子音楽配信システム1 0では、ユーザホームネットワーク5内に機器として、電子配信専用記録メディア2 5 1が着脱自在に設けられた記録再生装置2 5 0を設け、サービスプロバイダ3からコンテンツ鍵 $K_{co}$ で暗号化されているコンテンツ、個別鍵 $K_i$ で暗号化されているコンテンツ鍵 $K_{co}$ および配送鍵 $K_d$ で暗号化されている個別鍵 $K_i$ （すなわち、コンテンツプロバイダセキュアコンテナおよびサービスプロバイダセキュアコンテナ）が送信されると、記録再生装置2 5 0により電子配信専用記録メディア2 5 1を制御して購入処理を実行させ、当該電子配信専用記録メディア2 5 1において、コンテンツ鍵 $K_{co}$ で暗号化されているコンテンツを外部メモリ3 0 3に記録すると共に、配送鍵 $K_d$ で暗号化されている個別鍵 $K_i$ を当該配送鍵 $K_d$ で復号化し、個別鍵 $K_i$ で暗号化されているコンテンツ鍵 $K_{co}$ を当該個別鍵 $K_i$ で復号化し、この復号化したコンテンツ鍵 $K_{co}$ を電子配信専用記録メディア2 5 1固有の保存鍵 $K_{save}$ で暗号化して外部メモリ3 0 3に記録する。因みに、電子配信専用記録メディア2 5 1

では、保存鍵 $K_{save}$ を当該電子配信専用記録メディア251内の耐タンパ性を有する暗号処理部301の記憶モジュール311に保存している。

また、記録再生装置250は、再生処理時、電子配信専用記録メディア251を制御することにより、当該電子配信専用記録メディア251において、外部メモリ303からコンテンツ鍵 $K_c$ で暗号化されているコンテンツおよび保存鍵 $K_{save}$ で暗号化しているコンテンツ鍵 $K_c$ を読み出し、当該保存鍵 $K_{save}$ で暗号化しているコンテンツ鍵 $K_c$ を当該保存鍵 $K_{save}$ で復号化し、かくして、コンテンツ鍵 $K_c$ で暗号化されているコンテンツおよび復号化したコンテンツ鍵 $K_c$ を取り出す。そして、記録再生装置250は、暗号処理部262および伸張部263を用いて、コンテンツ鍵 $K_c$ で暗号化されているコンテンツを当該コンテンツ鍵 $K_c$ を用いて復号化する。

従って、電子音楽配信システム10では、記録再生装置250により、電子配信専用記録メディア251において、外部メモリ303にコンテンツ鍵 $K_c$ で暗号化されているコンテンツと、保存鍵 $K_{save}$ で暗号化したコンテンツ鍵 $K_c$ を記録するものの、当該電子配信専用記録メディア251からコンテンツ鍵 $K_c$ で暗号化されているコンテンツおよび復号化したコンテンツ鍵 $K_c$ を読み出すため、記録再生装置250に、その暗号処理部262固有の保存鍵を保持する必要がない。このため、電子音楽配信システム10では、記録再生装置250と同様な暗号処理部262および伸張部263を有すれば、電子配信専用記録メディア251にコンテンツを記録した記録再生装置250とは異なる他の機器でも、当該電子配信専用記録メディア251を用いてコンテンツを再生して利用することができ、かくして、電子配信専用記録メディア251の汎用性を格段的に向上させることができる。

また、電子配信専用記録メディア251では、仮に、外部メモリ303からコンテンツおよびコンテンツ鍵 $K_c$ が不当に読み出されたとしても、コンテンツを復号化するためのコンテンツ鍵 $K_c$ を暗号化する際に用いた保存鍵 $K_{save}$ を耐タンパ性を有する暗号処理部301内の記憶モジュール311に保持して、当該保存

鍵 $K_{save}$ が不当に読み出されることを防止することができ、かくして、コンテンツが不当に利用されることを防止することができる。

さらに、電子音楽配信システム10では、電子配信専用記録メディア251の汎用性を向上させる分、当該電子配信専用記録メディア251に記録したコンテンツに対して課金情報を回収するまでの間、当該コンテンツに対して利用を制限（再生や複製の回数または期間を制限）することにより、当該課金情報が回収されないまま、コンテンツが不当に利用されることを防止することができる。

以上の構成によれば、記録再生装置250に着脱自在に設けられた電子配信専用記録メディア251に当該電子配信専用記録メディア251固有の保存鍵 $K_{save}$ を保持し、購入処理時、記録再生装置250がコンテンツ鍵 $K_c$ で暗号化されているコンテンツ、個別鍵 $K_i$ で暗号化されているコンテンツ鍵 $K_c$ および配送鍵 $K_d$ で暗号化されている個別鍵 $K_i$ を電子配信専用記録メディア251に送信して当該電子配信専用記録メディア251において、コンテンツ鍵 $K_c$ で暗号化されたコンテンツを外部メモリ303に記録すると共に、暗号化されている個別鍵 $K_i$ を配送鍵 $K_d$ で復号化した後、暗号化されているコンテンツ鍵 $K_c$ をこの個別鍵 $K_i$ で復号化し、得られたコンテンツ鍵 $K_c$ を保存鍵 $K_{save}$ で暗号化して外部メモリ303に記録し、再生処理時、記録再生装置250が電子配信専用記録メディア251からコンテンツ鍵 $K_c$ で暗号化されたコンテンツと、保存鍵 $K_{save}$ で復号化されたコンテンツ鍵 $K_c$ を取り出すようにして当該コンテンツを復号化するようにしたことにより、当該電子配信専用記録メディア251をコンテンツの記録に用いた記録再生装置250とは異なる他の記録再生装置250に挿入した場合でも、この電子配信専用記録メディア251からコンテンツを再生することができ、かくして電子配信専用記録メディア251の汎用性を格段的に向上し得る電子音楽配信システムを実現することができる。

因みに、かかる電子音楽配信システム10では、電子配信専用記録メディア251に配送鍵 $K_d$ を保持せず、または配送鍵 $K_d$ を保持していても使用しないようにし、記録再生装置250により、コンテンツの記録時、個別鍵 $K_i$ で暗号化

されているコンテンツ鍵 $K_{co}$ を当該個別鍵 $K_i$ で復号化した後、当該コンテンツ鍵 $K_{co}$ を電子配信専用記録メディア251との間で相互認証して共有化した一時鍵 $K_{temp}$ を用いて暗号化し、当該一時鍵 $K_{temp}$ で暗号化したコンテンツ鍵 $K_{co}$ をコンテンツ鍵 $K_{co}$ で暗号化されているコンテンツと共に、当該電子配信専用記録メディア251に送信するようにしても良い。

また、本発明においては、情報送信装置として、コンテンツプロバイダ2を適用したが、当該情報送信装置として、コンテンツプロバイダ2およびサービスプロバイダ3を適用しても良い。

#### (8) 課金情報の代理処理および利用権の管理移動処理

図92について上述した電子配信専用記録メディア251は、電子配信サービスセンタ1に接続される機器として、例えば、図15について上述したデータ管理システムであるユーザホームネットワーク5内の管理装置であるホームサーバ51に挿入されることにより、暗号処理部301の記憶モジュール311に保持している課金情報をこのホームサーバ51に送信し、かくして、課金情報をホームサーバ51から電子配信サービスセンタ1に回収させ得るようになされている。

これにより、電子配信専用記録メディア251においては、課金情報を保持していると、コンテンツの不正利用を防止するうえで、当該コンテンツと共にその利用権（このコンテンツを再生するための権利）を他の機器に移動（制限付き移動、管理移動）したり、または削除（削除は、課金処理が済んでいないと実行することはできない）することができないものの、このように、課金情報をホームサーバ51に送信すると、当該課金情報に対応するコンテンツと共にその利用権を、図82について上述した管理移動権の移動処理手順に従って、他の機器に移動（制限付き移動、管理移動）させることができる。

ところで、電子配信専用記録メディア251から他の機器にコンテンツと共に利用権を移動すると、当該コンテンツおよびその利用権を取得した機器は、当該コンテンツおよびその利用権を必要に応じて電子配信専用記録メディア251に

のみ戻すことができる。しかしながら、電子配信専用記録メディア 251 は、自由に持ち運びできるため、他の機器からコンテンツおよびその利用権を容易には戻し難い場合がある。

従って、電子配信サービスセンタ 1 に接続されたユーザホームネットワーク 5 内の機器として、例えば、ホームサーバ 51 (図 15) においては、電子配信専用記録メディア 251 に保持している課金情報を取り込む際、当該電子配信専用記録メディア 251 から対応するコンテンツやその利用権も合わせて取り込み、この電子配信専用記録メディア 251 に代わり、当該取り込んだコンテンツおよび利用権を管理するようにした。

実際に、ホームサーバ 51 において実行される課金情報の代理処理、およびコンテンツを再生するための権利 (利用権) の移動 (制限付き移動、管理移動) について、図 95 に示すフローチャートを用いて説明する。ステップ S740 において、ホームサーバ 51 においては、電子配信専用記録メディア 251 が挿入され、この状態において、ユーザが入力手段 63 を介して課金情報の代理処理および利用権の移動処理の実行命令を入力すると、上位コントローラ 62 が当該ホームサーバ 51 および電子配信専用記録メディア 251 を制御することにより、ホームサーバ 51 内の暗号処理部 65 の制御部 91 が、電子配信専用記録メディア 251 内の暗号処理部 301 との間で、互いの相互認証モジュール 95 および 314 を用いて相互認証し、一時鍵  $K_{temp}$  を共有化する。

次いで、ステップ S741 において、電子配信専用記録メディア 251 内の暗号処理部 301 の制御部 310 は、記憶モジュール 311 に保持している課金情報を暗号/復号化モジュール 315 内の暗号化ユニット 321 に送出し、当該暗号化ユニット 321 において、一時鍵  $K_{temp}$  で課金情報を暗号化し、当該暗号化した課金情報を署名生成ユニット 323 に送出する。

また、暗号処理部 301 の制御部 310 は外部メモリ制御部 302 を介して外部メモリ 303 から、課金情報に含まれるコンテンツプロバイダの ID、取扱方針の ID および取扱方針のバージョンに対応する取扱方針と、当該課金情報に含

まれるサービスプロバイダのID、価格情報のIDおよび価格情報のバージョンに対応する価格情報を読み出し、当該読み出した取扱方針および価格情報を署名生成ユニット323に送出する。これにより、暗号処理部301の制御部310は、署名生成ユニット323において、一時鍵 $K_{temp}$ で暗号化されている課金情報および取扱方針並びに価格情報全体に対して（または個別に対して）署名を付加し、当該署名を付加した課金情報および針扱方針並びに価格情報を通信部300を介してホームサーバ51の上位コントローラ62に送信する。

因みに、電子配信専用記録メディア251においては、課金情報が送信途中に改竄されると、第3者が不当に利益を得たりするため、当該課金情報には必ず署名を付加し、改竄されていないか否かを調べるようにする。また、課金情報は、その内容が見られても特に支障はないため、暗号化せずに送信しても良い。ホームサーバ51においては、取扱方針および価格情報を用いなくとも課金情報の代理処理および利用権の移動処理を実行し得る。従って、電子配信専用記録メディア251においては、ホームサーバ51に取扱方針および価格情報を必要に応じて送信すれば良い。

ステップS742において、ホームサーバ51の上位コントローラ62は、電子配信専用記録メディア251から送信された課金情報および取扱方針並びに価格情報を暗号処理部65の制御部91に送出する。これにより、制御部91は、暗号／復号化モジュール96内の署名検証ユニット115において、課金情報および取扱方針並びに価格情報に付加された署名を検証し、これらが改竄されていなければ、復号化ユニット111において、一時鍵 $K_{temp}$ で暗号化されている課金情報を当該一時鍵 $K_{temp}$ で復号化する。

次いで、ステップS743において、電子配信専用記録メディア251内の暗号処理部301の制御部310は、このとき、ステップS742において、記憶モジュール311内に保持している課金情報（ステップS741でホームサーバ51に送信した課金情報であり、記憶モジュール311内において削除しない限りはそのまま残っている）が示すコンテンツのIDを検索し、当該検索したコン

テンツのIDに基づいて、外部メモリ制御部302を介して外部メモリ303から、対応する全ての使用許諾条件情報およびコンテンツ鍵 $K_c$ で暗号化されているコンテンツを読み出す。

暗号処理部301の制御部310は、当該読み出したコンテンツ鍵 $K_c$ を暗号／復号化モジュール315の復号化ユニット320に送出することにより、当該復号化ユニット320において、保存鍵 $K_{save}$ で暗号化されているコンテンツ鍵 $K_c$ を、記憶モジュール311に保持している保存鍵 $K_{save}$ で復号化し、続いて、暗号化ユニット321において、この復号化したコンテンツ鍵 $K_c$ を一時鍵 $K_{temp}$ で暗号化する。そして、制御部310は、外部メモリ303から読み出した使用許諾条件情報および暗号化されているコンテンツと共に、一時鍵 $K_{temp}$ で暗号化しているコンテンツ鍵 $K_c$ に署名生成ユニット323において署名を付加した後、通信部300を介してホームサーバ51に送信する。因みに、署名は、使用許諾条件情報、コンテンツ、コンテンツ鍵 $K_c$ それぞれ個別に付加しても良く、また、これら使用許諾条件情報、コンテンツおよびコンテンツ鍵 $K_c$ 全体を1つにして付加しても良い。さらに、コンテンツには署名を付加しない場合もある。

続いて、ステップS744において、ホームサーバ51内の暗号処理部65の制御部91は、電子配信専用記録メディア251から送信された使用許諾条件情報および暗号化されているコンテンツ並びに一時鍵 $K_{temp}$ で暗号化しているコンテンツ鍵 $K_c$ を上位コントローラ62を介して取り込み、署名検証ユニット115において、この使用許諾条件情報および暗号化されているコンテンツ並びに一時鍵 $K_{temp}$ で暗号化しているコンテンツ鍵 $K_c$ に付加されている署名を検証した後、これらが改竄されていなければ、復号化ユニット111において、一時鍵 $K_{temp}$ で暗号化されているコンテンツ鍵 $K_c$ を当該一時鍵 $K_{temp}$ で復号化する。

これにより、ステップS745において、ホームサーバ51内の上位コントローラ62は、暗号処理部65から得られる、コンテンツ鍵 $K_c$ で暗号化されているコンテンツ（ステップS744で署名検証したコンテンツ）と、必要に応じて得られる取扱方針および価格情報（ステップS742で署名検証した取扱方針お

および価格情報)とを大容量記憶部68に保存する。因みに、ステップS745において、実行される大容量記憶部68への記録処理は、ステップS741およびステップS743において、データが送信された直後に実行しても良い。

また、ステップS746において、ホームサーバ51内の暗号処理部65の制御部91は、課金情報(ステップS742で署名検証した課金情報)を記憶モジュール92に保存すると共に、使用許諾条件情報(ステップS744で署名検証した使用許諾条件情報)に格納されている暗号処理部のID(コンテンツを購入処理した機器の暗号処理部のID)を自己のもの(すなわち、ホームサーバ51内の暗号処理部65のID)に変更して当該使用許諾条件情報を更新する。

次いで、ステップS747において、ホームサーバ51内の暗号処理部65の制御部91は、暗号/復号化モジュール96内の暗号化ユニット112において、コンテンツ鍵 $K_{co}$ 。(ステップS744で復号化したコンテンツ鍵 $K_{co}$ )を、記憶モジュール92に保持している保存鍵 $K_{save}$ で暗号化し、当該暗号化したコンテンツ鍵 $K_{co}$ と共に使用許諾条件情報(ステップS746で更新した使用許諾条件情報)を外部メモリ制御部97を介して外部メモリ67に保存する。因みに、外部メモリ67における、データ書込み時の改竄チェックについては、図69について上述した処理手順と同様に実行されるため、その説明は省略する。

そして、ステップS748において、ホームサーバ51内の暗号処理部65の制御部91は、このように、電子配信専用記録メディア251から送信された、課金情報、暗号化されているコンテンツ、コンテンツ鍵 $K_{co}$ 、使用許諾条件情報、取扱方針および価格情報をそれぞれ保存すると、課金情報の代理処理および利用権の移動が完了したことを示す処理完了データを上位コントローラ62を介して電子配信専用記録メディア251に送信する。

これにより、ステップS749において、電子配信専用記録メディア251内の暗号処理部301の制御部310は、ホームサーバ51から送信された処理完了データを受信すると、外部メモリ制御部302を介して外部メモリ303内の、コンテンツ鍵 $K_{co}$ で暗号化されているコンテンツ、保存鍵 $K_{save}$ で暗号化されて



いるコンテンツ鍵 $K_c$ 。および使用許諾条件情報（すなわち、ステップS 7 4 3でホームサーバ5 1に送信したものである）と、必要に応じて取扱方針および価格情報（すなわち、ステップS 7 4 2でホームサーバ5 1に送信したものである）をそれぞれ削除する。因みに、外部メモリ3 0 3におけるデータ削除時の改竄チェックは、図7 1について上述した処理手順と同様に実行されるため、その説明は省略する。

これに加えて、ステップS 7 5 0において、電子配信専用記録メディア2 5 1内の暗号処理部3 0 1の制御部3 1 0は、記憶モジュール3 1 1内の課金情報（すなわち、ステップS 7 4 1でホームサーバ5 1に送信したものである）を削除し、かくしてこの処理手順を終了する。

以上のように、電子配信専用記録メディア2 5 1においては、暗号処理部3 0 1内の記憶モジュール3 1 1に保持している課金情報と共に、対応するコンテンツやコンテンツ鍵 $K_c$ 。、さらには使用許諾条件情報をホームサーバ5 1に送信する共に、この際、ホームサーバ5 1に送信した課金情報、コンテンツ、コンテンツ鍵 $K_c$ 。および使用許諾条件情報を内部の記憶モジュール3 1 1や、外部メモリ3 0 3から削除することにより、当該コンテンツをホームサーバ5 1に管理させるようにする。

そして、ホームサーバ5 1においては、電子配信専用記録メディア2 5 1からコンテンツを取り込んだ際、当該コンテンツと共に取り込んだ使用許諾条件情報の暗号処理部のIDを変更し、このコンテンツの所有者をホームサーバ5 1自体にしたため、図8 2について上述した管理移動権の移動処理手順に従って、コンテンツを他の機器に移動させることができると共に、図8 3について上述した管理移動権の返還処理手順に従って、各機器から返還されるコンテンツを取り込むことができる。

以上の構成において、電子音楽配信システム1 0では、記録装置である記録再生装置2 5 0を用いて電子配信専用記録メディア2 5 1により購入処理を実行させ、当該電子配信専用記録メディア2 5 1において、コンテンツと共に、そのコ

コンテンツを再生させるための権利、使用許諾条件情報および課金情報を保持させる。そして、電子配信専用記録メディア251が保持する課金情報を電子配信サービスセンタ1に回収させるために、当該電子配信専用記録メディア251がユーザホームネットワーク5内のホームサーバ51に挿入されると、当該ホームサーバ51は、電子配信専用記録メディア251に保持している課金情報と共に、対応するコンテンツ、利用権および使用許諾条件情報を取り込むようにして当該コンテンツを電子配信専用記録メディア251に代えて管理する。

従って、電子音楽配信システム10では、ユーザホームネットワーク5内において、ホームサーバ51が電子配信専用記録メディア251から管理を引き受けたコンテンツと共にその利用権を、当該ユーザホームネットワーク5内の他の機器や、記録メディア、また、電子配信専用記録メディア251に管理移動することができると共に、これらユーザホームネットワーク5内の他の機器、記録メディアおよび電子配信専用記録メディア251が当該コンテンツをホームサーバ51に返還することができ、かくして、電子配信専用記録メディア251において購入処理して取得したコンテンツを、ホームサーバ51の管理の元に、ユーザホームネットワーク5内の他の機器、記録メディアおよび当該電子配信専用記録メディア251に用いて容易に利用することができる。

また、電子配信専用記録メディア251では、課金情報を保持していると、購入した利用権に制限が付加されるため、当該課金情報を電子配信サービスセンタ1に接続されたホームサーバ51によって回収する必要がある。そして、電子配信専用記録メディア251では、かかる課金情報の回収の際に、対応するコンテンツの管理をホームサーバ51に移行すれば、外部メモリ302において空き領域を確保し易くなり、かくして、コンテンツを購入処理する際に、既に保持しているコンテンツを削除して無駄にすることを防止することができる。

さらに、ユーザホームネットワーク5では、このように、ホームサーバ51により、電子配信専用記録メディア251において購入処理して取得したコンテンツを保管して管理するため、当該電子配信専用記録メディア251に保持し得る

コンテンツ（すなわち、外部メモリ 303 の記憶容量に依存する）以上のコンテンツを容易に所有することができる。

以上の構成によれば、記録再生装置 250 を用いて電子配信専用記録メディア 251 において購入処理して保持したコンテンツをその課金情報と共にユーザホームネットワーク 5 内のホームサーバ 51 に移動させ、当該ホームサーバ 51 においてこのコンテンツを保管も兼ねて管理するようにしたことにより、当該ホームサーバ 51 が電子配信専用記録メディア 251 から管理を引き受けたコンテンツを、ユーザホームネットワーク 5 内の他の機器や、記録メディア、また、電子配信専用記録メディア 251 に管理移動することができ、かくして電子配信専用記録メディア 251 に記録したコンテンツを、ユーザホームネットワーク 5 内の他の機器や、記録メディア等の各種機器によって容易に利用し得る電子音楽配信システムを実現することができる。

#### （9）オンライン課金購入処理

かかる電子音楽配信システム 10 においては、情報規制装置である電子配信サービスセンタ 1 と、情報送信装置であるサービスプロバイダ 3 との間をネットワークを介してオンライン接続すると共に、当該サービスプロバイダ 3 と、ユーザホームネットワーク 5（実際には情報受信装置であるホームサーバ 51）との間もネットワークを介してオンライン接続してシステム構築し得るようになされている。

そして、このように電子音楽配信システム 10 を構築した場合の全体を通したデータの流れを図 96 に示す。コンテンツプロバイダ 2 からサービスプロバイダ 3 へのデータの送信と、当該サービスプロバイダ 3 からユーザホームネットワーク 5 へのデータの送信については、図 20 について上述したデータの流れと同様であるため、その詳細な説明は省略する。

ユーザホームネットワーク 5（ホームサーバ 51）は、課金情報を暗号化し、当該暗号化した課金情報に署名を付加して、サービスプロバイダ 3 を介して電子配信サービスセンタ 1 に送信する。因みに、購入処理に用いた取扱方針および価

格情報には、決済に必要な情報等のように電子配信サービスセンタ 1 において必要とされる情報が含まれているものの、これら各種情報は課金情報にも含まれているため、ユーザホームネットワーク 5（ホームサーバ 5 1）は、購入処理の際に取扱方針および価格情報を電子配信サービスセンタ 1 にはとくに送信しないようになされている。

また、電子配信サービスセンタ 1 およびユーザホームネットワーク 5 間では、サービスプロバイダ 3 を介して、配送鍵  $K_d$  および登録情報（図示せず）の更新も行うようになされている。これにより、ユーザホームネットワーク 5 は、図 1 について上述したシステムの構築例に比べて、サービスプロバイダ 3 および電子配信サービスセンタ 1 とのデータの通信の際に、使用する通信経路を切り換える必要がなく、通信部の処理を軽減させ得る。

因みに、ユーザホームネットワーク 5（ホームサーバ 5 1）と、電子配信サービスセンタ 1 との間でデータの送受信を行う場合、サービスプロバイダ 3 は、ユーザホームネットワーク 5（ホームサーバ 5 1）および電子配信サービスセンタ 1 間のデータの通信路として使用され、当該データを改竄することができないようになされている。

ここで、ユーザホームネットワーク 5 内のホームサーバ 5 1 においては、購入処理により生成した課金情報を暗号処理部 6 5 内の記憶モジュール 9 2 に保存しておき、当該保存している課金情報（複数の場合もある）を所定のタイミングで電子配信サービスセンタ 1 に一括して送信する場合と、購入処理しながら、このとき生成した課金情報を電子配信サービスセンタ 1 に送信する場合がある。因みに、購入処理しながら、このとき生成した課金情報を電子配信サービスセンタ 1 に送信するオンライン課金購入処理は、取扱方針または価格情報に当該オンライン課金購入処理を実行するか否かが記述されている場合がある。

ホームサーバ 5 1 において、実行されるオンライン課金購入処理を、図 9 7 に示すフローチャートを用いて説明する。ステップ S 7 6 0 において、ホームサーバ 5 1 内の暗号処理部 6 5 の制御部 9 1 は、上位コントローラ 6 2 の制御のもと

に、記憶モジュール 9 2 に記憶されている配送鍵  $K_d$  の有効期限（バージョン）を判定し、当該搬送鍵  $K_d$  が有効である場合にはステップ S 7 6 1 に進む。

ステップ S 7 6 1 において、暗号処理部 6 5 の制御部 9 1 は、記憶モジュール 9 2 に記憶されている課金情報の課金の合計が予め設定された上限に達しているか否かを判断し、当該課金の合計が上限に達していない場合にはステップ S 7 6 2 に進む。因みに、暗号処理部 6 5 の制御部 9 1 は、購入処理しながら、このとき生成した課金情報を電子配信サービスセンタ 1 に送信する場合には、当該課金情報を記憶モジュール 9 2 に保存しないため、このステップ S 7 6 1 の処理を実行せずにステップ S 7 6 2 に進む。

ステップ S 7 6 2 乃至ステップ S 7 6 6 は、図 6 7 について上述したステップ S 1 6 2 乃至ステップ S 1 6 9 と順次同様の処理を実行するため、その詳細な説明は省略する。ステップ S 7 6 7 において、ホームサーバ 5 1 の上位コントローラ 6 2 は、表示手段 6 4 を用いて購入可能なコンテンツの情報（例えば、購入可能な利用形態や価格など）を表示し、これによりユーザが入力手段 6 3 を用いて購入項目を選択し得る。そして、入力手段 6 3 から入力された信号はホームサーバ 5 1 の上位コントローラ 6 2 に送出され、当該上位コントローラ 6 2 は、その信号に基づいて購入コマンドを生成し、当該購入コマンドを暗号処理部 6 5 の制御部 9 1 に送出する。因みに、このような入力処理はオンライン課金購入処理のスタート時に行っても良い。

暗号処理部 6 5 の制御部 9 1 は、上位コントローラ 6 2 から購入コマンドが与えられると、ステップ S 7 6 4 において署名検証した取扱方針およびステップ S 7 6 6 において署名検証した価格情報に基づいて、課金情報および使用許諾条件情報を生成する。因みに、制御部 9 1 は、この際、暗号処理部 6 5 内に設けられたデータ処理実行用の RAM（Random Access Memory）を用いて、課金情報および使用許諾条件情報を生成し、当該生成した課金情報および使用許諾条件情報を RAM にそのまま保持しておく。

次いで、ステップ S 7 6 8 において、ホームサーバ 5 1 内の暗号処理部 6 5 の

制御部 9 1 は、相互認証モジュール 9 5 を用いて、電子配信サービスセンタ 1 の相互認証部 1 7 との間で相互認証し、当該電子配信サービスセンタ 1 との間で一時的鍵  $K_{temp}$  を共有化する。

続いて、ステップ S 7 6 9 において、ホームサーバ 5 1 内の暗号処理部 6 5 の制御部 9 1 は、暗号／復号化モジュール 9 6 の暗号化ユニット 1 1 2 を用いて、課金情報を一時的鍵  $K_{temp}$  で暗号化した後、署名生成ユニット 1 1 4 を用いて署名を付加して、サービスプロバイダ 3 を介して電子配信サービスセンタ 1 に送信する。因みに、ホームサーバ 5 1 は、電子配信サービスセンタ 1 への送信に先立って課金情報を一時的鍵  $K_{temp}$  で暗号化したが、これは、コンテンツを購入するユーザのプライバシーを保護するためである。また、ホームサーバ 5 1 は、課金情報を暗号化せずに署名を付加して電子配信サービスセンタ 1 に送信する場合もある。

ステップ S 7 7 0 において、電子配信サービスセンタ 1 は、ホームサーバ 5 1 から送信された一時的鍵  $K_{temp}$  で暗号化されている課金情報を受信すると、当該課金情報に付加されている署名を検証し、当該課金情報が改竄されていなければ、この一時的鍵  $K_{temp}$  で暗号化されている課金情報を、ホームサーバ 5 1 と共有化している一時的鍵  $K_{temp}$  を用いて復号化し、かくして、復号化した課金情報を経歴データ管理部 1 5 に保存する。

そして、ステップ S 7 7 1 において、電子配信サービスセンタ 1 は、このように、課金情報を保存すると、当該課金情報を受領したことを示す受領データを生成し、当該生成した受領データに署名を付加して、サービスプロバイダ 3 を介してホームサーバ 5 1 に送信する。これにより、ホームサーバ 5 1 内の暗号処理部 6 5 の制御部 9 1 は、電子配信サービスセンタ 1 から送信された受領データを通信部 6 1 および上位コントローラ 6 2 を順次介して取り込み、受領データに付加されている署名を署名検証ユニット 1 1 5 で検証し、当該受領データが改竄されていなければ、RAM に保持していた課金情報を消去し、ステップ S 7 7 2 に進む。

ステップ S 7 7 2 乃至ステップ S 7 7 4 は、図 6 7 について上述したステップ

S 1 7 2乃至ステップS 1 7 4と順次同様の処理を実行するため、その詳細な説明は省略する。因みに、ステップS 7 7 2乃至ステップS 7 7 4はどのような順番で実行しても良い。また、ステップS 7 7 5において実行される登録情報更新処理は、図6 1および図6 2について上述した登録情報更新処理と同様なため、その詳細な説明は省略する。さらに、ステップS 7 7 6は、図6 7について上述したステップS 1 7 6と同様にエラー処理を実行するため、その詳細な説明は省略する。ところで、かかるオンライン課金購入処理では、コンテンツ鍵 $K_c$ で暗号化されているコンテンツ、取扱方針および価格情報が、これらに付加された署名が検証された後のいずれかのステップにおいて、外部メモリ制御部9 7に介して外部メモリ6 7に保持される。

ところで、ステップS 7 7 0において、電子配信サービスセンタ1は、課金情報の署名を検証した結果、当該課金情報が改竄されるなどして不当なデータであると判断すると、当該課金情報を経歴データ管理部に保存しないようにする。そして、ステップS 7 7 1において、電子配信サービスセンタ1は、課金情報が不当なデータであるために受領しないことを示す受領拒否データを生成し、これを、サービスプロバイダ3を介してホームサーバ5 1に送信する。このとき、ホームサーバ5 1の上位コントローラ6 2は、電子配信サービスセンタ1から送信された受領拒否データが通信部6 1によって受信されると、当該受領拒否データに基づいて、暗号処理部6 5の制御部9 1に購入処理を中断させると共に、ユーザが購入しようとしているコンテンツが購入できないことを表示手段6 4を介してユーザに報知する。

このように、ホームサーバ5 1において実行されるオンライン課金購入処理においては、購入処理途中に電子配信サービスセンタ1がその購入処理を許可したときのみコンテンツを購入し得る。なお、本実施の形態では、電子配信サービスセンタ1が受領データおよび受領拒否データをそのまま送信しているが、一時鍵 $K_{temp}$ で暗号化した後、署名を付加して送信し、ホームサーバ5 1では、暗号化されている受領データおよび受領拒否データに付加された署名を検証した後、当該

暗号化されている受領データおよび受領拒否データを一時鍵 $K_{temp}$ で復号化して、その復号化した受領データおよび受領拒否データに基づいて、課金情報が回収されたか否かを確認するようにしても良い。

以上の構成において、電子音楽配信システム10では、ホームサーバ51において、オンライン課金購入処理を実行した場合、当該購入処理途中に、電子配信サービスセンタ1がホームサーバ61から送信された課金情報を受信し、当該課金情報に付加されている署名を検証することによりこの課金情報が不当なデータであるか否かを判断し、この結果、課金情報を正当なデータであると判断したときには（すなわち、ホームサーバ51が受領データを受信したときには）、ホームサーバ51において、購入処理を継続して実行させてコンテンツを購入させる。

これに対して、電子音楽配信システム10では、ホームサーバ51において実行される購入処理途中に、電子配信サービスセンタ1が課金情報を不当なデータであると判断したときには（すなわち、ホームサーバ51が受領拒否データを受信したときには）、ホームサーバ51において、この購入処理を中断させ、コンテンツの購入を禁止する。

従って、電子音楽配信システム10では、ホームサーバ51から電子配信サービスセンタ1に送信される課金情報が改竄され（暗号処理部65の外部や、ホームサーバ51と電子配信サービスセンタ1との間の通信経路において課金情報が改竄され）、例えば、購入対象のコンテンツが他のコンテンツに変更されていたり、またはコンテンツの利用権が他の利用権に変更されている場合でも、これら不当なコンテンツや、不当な利用権が購入されることを未然に防止することができる。

また、ホームサーバ51から電子配信サービスセンタ1に送信される課金情報が改竄され、例えば、コンテンツの価格、またはコンテンツの購入に伴う利益の分配先が変更されている場合にも、当該コンテンツが不当な価格で購入されたり、または第3者が不当に利益を得ることを未然に防止することができる。

以上の構成によれば、電子配信サービスセンタ1と、ユーザホームネットワー



ク 5 とをネットワークを介してオンライン接続し、当該ホームサーバ 5 1 が購入処理の実行途中にこのとき生成した課金情報を電子配信サービスセンタ 1 に送信し、当該電子配信サービスセンタ 1 がこの課金情報が正当なデータであるか否かを判断し、当該課金情報が不当なデータであると判断したときには、ホームサーバ 5 1 に購入処理を中断させてコンテンツを購入させないようにしたことにより、課金情報が改竄されてコンテンツや、その利用権が不当に購入されることを未然に防止することができ、かくしてコンテンツが不当に利用されることを防止し得る電子音楽配信システムを実現することができる。

因みに、電子配信サービスセンタ 1 は、ホームサーバ 5 1 から送信された課金情報に基づいて、コンテンツの購入を許可するか否かを判断したが、ホームサーバ 5 1 から使用許諾条件情報のように、ユーザが購入しようとするコンテンツおよびまたは利用権を記述した利用許可データを電子配信サービスセンタ 1 に送信し、当該電子配信サービスセンタ 1 がこの利用許可データに基づいてコンテンツの購入や、利用を許可するか否かを判断しても良い。

#### (10) 情報提供装置の構成

図 1 との対応部分に同一符号を付して示す図 9 8 において、かかる構成の電子音楽配信システム 10 には、情報提供装置 330 が設けられている。情報提供装置 330 は、コンテンツプロバイダ 2 から供給される暗号化された多数のコンテンツを保持するホスティングサーバ 331 と、例えば、簡易小売店（すなわち、KIOSK）に設置される情報提供端末（以下、これを KIOSK 端末と呼ぶ）332 とから構成される。

KIOSK 端末 332 においては、例えば、MD（商標）でなる記録媒体である記録メディア 333 や、図 17 について上述したデータ格納装置である電子配信専用記録メディア 334 を着脱自在に挿入し得る。そして、KIOSK 端末 332 は、当該 KIOSK 端末 332 を管理する情報提供者側（図 1 でのサービスプロバイダ 3）で作成した価格情報を保持し、また、専用のケーブルまたは衛星通信を介してホスティングサーバ 331 から情報利用者である顧客の所望するコ

ンテンツを読み出し、ユーザホームネットワーク 5 内のホームサーバ 5 1 と同様に購入処理を実行することにより、顧客の所持する記録メディア 3 3 3 や、電子配信専用記録メディア 3 3 4 に当該顧客が所望するコンテンツを記録する。

因みに、K I O S K 端末 3 3 2 は、電子配信サービスセンタ 1 から送信される K I O S K 端末 3 3 2 の公開鍵証明書、配送鍵  $K_d$ 、登録情報等を受信し、これに対して電子配信専用記録メディア 3 3 4 にコンテンツの利用権に応じた課金情報や、使用許諾条件情報等を送信する。これにより、電子配信サービスセンタ 1 は、K I O S K 端末 3 3 2 から与えられる課金情報に基づいて、コンテンツプロバイダ 2 や情報提供者（図 1 でのサービスプロバイダ 3）らに対しても利益配分の処理を行う。また、電子配信専用記録メディア 3 3 4 は、K I O S K 端末 3 3 2 から利用権を購入する際に当該電子配信専用記録メディア 3 3 4 内で購入処理する場合があり、この場合にはユーザホームネットワーク 5 内の機器等を介して電子配信サービスセンタ 1 に課金情報を送信する必要がある。

ここで、図 9 9 はホスティングサーバ 3 3 1 の構成を示すものである。ホスティングサーバ 3 3 1 は、通信部 3 4 0、制御部 3 4 1 およびサーバ 3 4 2 から構成される。通信部 3 4 0 は、コンテンツプロバイダ 2 および K I O S K 端末 3 3 2 と通信し、所定の情報を送受信する。制御部 3 4 1 は、通信部 3 4 0 およびサーバ 3 4 2 を制御することによりコンテンツプロバイダ 2 からコンテンツプロバイダセキュアコンテナが送信されると、当該コンテンツプロバイダセキュアコンテナに含まれる暗号化されたコンテンツをサーバ 3 4 2 に保持すると共に、当該コンテンツプロバイダセキュアコンテナに含まれる鍵データや取扱方針等を通信部 3 4 0 を介して K I O S K 端末 3 3 2 に送信する。

また、制御部 3 4 1 は、K I O S K 端末 3 3 2 からコンテンツの読出要求コマンドが与えられると、サーバ 3 4 2 から対応するコンテンツを読み出し、当該読み出したコンテンツを通信部 3 4 0 を介して K I O S K 端末 3 3 2 に送信する。因みに、コンテンツの読出要求コマンドの通信経路と、コンテンツの通信経路は異なっていることがある。

図100は、KIOSK端末332の構成を示すものであり、当該KIOSK端末332は、受信手段である通信部350、KIOSK端末332を制御する格納手段である上位コントローラ351、使用許諾条件情報作成手段である暗号処理部352、電子透かし挿入手段である電子透かし挿入部353、代金処理部354、入力手段355、表示手段356、コンテンツ記録手段であるKIOSK端末サーバ357から構成される。

通信部350は、ホスティングサーバ331や、電子配信サービスセンタ1と通信し、所定の情報を送受信する。上位コントローラ351は、ホームサーバ51の上位コントローラ62と同様の機能を有することによりその説明は省略する。暗号処理部352は、制御部360、記憶モジュール361、登録情報検査モジュール362、購入処理モジュール363、相互認証モジュール364および暗号／復号化モジュール365から構成される。これら制御部360、記憶モジュール361、登録情報検査モジュール362、購入処理モジュール363、相互認証モジュール364は、それぞれホームサーバ51の対応する制御部91、記憶モジュール92、登録情報検査モジュール93、購入処理モジュール94、相互認証モジュール95と同様の機能を有することによりその説明は省略する。

暗号／復号化モジュール365は、復号化ユニット370、暗号化ユニット371、乱数発生ユニット372、署名生成ユニット373および署名検証ユニット374から構成される。これら復号化ユニット370、暗号化ユニット371、乱数発生ユニット372、署名生成ユニット373および署名検証ユニット374は、それぞれホームサーバ51の暗号／復号化モジュール96の対応する復号化ユニット111、暗号化ユニット112、乱数発生ユニット113、署名生成ユニット114および署名検証ユニット115と同様の機能を有することにより、その説明を省略する。

電子透かし挿入部353は、相互認証モジュール380、鍵復号化モジュール381、復号化モジュール382、電子透かし付加モジュール383および記憶モジュール384から構成される。この電子透かし挿入部353においては、相

互認証モジュール380、鍵復号化モジュール381、復号化モジュール382、電子透かし付加モジュール383および記憶モジュール384が、それぞれホームサーバ51の伸張部62の対応する相互認証モジュール101、鍵復号化モジュール102、復号化モジュール103、電子透かし付加モジュール105および記憶モジュール106と同様の機能を有するものの、コンテンツ鍵で復号化したコンテンツを伸張せずに、当該コンテンツに例えば、KIOSK端末332の所有者のIDを挿入してそのまま（デジタルデータのまま）記録メディア333や電子配信専用記録メディア334に送出する。ただし、電子透かし挿入部353においては、必要に応じて復号化モジュール382の出力であるコンテンツを伸張し、別の圧縮アルゴリズムを用いて再圧縮を行い、その出力を電子透かし付加モジュール383へ送出することもある。

代金処理部354は、購入処理の際に顧客が購入したコンテンツの利用権に対する代金の情報を表示手段356に表示し、KIOSK端末332に設けられた代金投入口から代金が投入されると、当該投入された代金に不足があるか否かを判断し、当該代金が不足している場合には、この不足金額の情報を表示手段356を介して顧客に通知すると共に、代金が多い場合には釣り銭の金額の情報を表示手段356を介して通知し、かつ代金返却口から釣り銭を返却する。

入力手段355は、操作ボタンを介して入力されるコンテンツの選択情報等の各種情報を上位コントローラ351に送出する。表示手段356は、液晶表示器のように所定の表示デバイスによって構成され、顧客に指示を出したり、情報を表示する。因みに、入力手段355および表示手段356は、タッチパネル式液晶表示器等により1つにまとめて構成することができる。

KIOSK端末サーバ357は、ホームサーバ51の大容量記憶部68と同様の機能を有し、ホスティングサーバ331から送信される鍵データ（暗号化されたコンテンツ鍵 $K_c$ 、暗号化された個別鍵 $K_i$ （図示せず）、取扱方針、およびKIOSK側で作成された価格情報等を保持する。因みに、KIOSK端末サーバ357は、暗号化されているコンテンツを保持する場合もある。

そして、K I O S K 端末 3 3 2 においては、当該 K I O S K 端末 3 3 2 に設けられたメディア挿入口に顧客が記録メディア 3 3 3 または電子配信専用記録メディア 3 3 4 を挿入すると、表示手段 3 5 6 を介してコンテンツの購入案内や、購入可能なコンテンツの情報等を表示し、この結果、顧客が入力手段 3 5 5 を介して所望するコンテンツを選択指定すると、当該選択指定されたコンテンツをホスティングサーバ 3 3 1 から読み出して購入処理し、このコンテンツを記録メディア 3 3 3 または電子配信専用記録メディア 3 3 4 に記録する。

因みに、図 1 0 1 は、コンテンツプロバイダ 2、ホスティングサーバ 3 3 1 および K I O S K 端末 3 3 2 の間で送信される情報を説明する図である。コンテンツプロバイダ 2 は、コンテンツプロバイダセキュアコンテナに当該コンテンツプロバイダの公開鍵証明書を付加してホスティングサーバ 3 3 1 に送信する。

ホスティングサーバ 3 3 1 は、コンテンツプロバイダ 2 の公開鍵証明書を検証し、当該コンテンツプロバイダ 2 の公開鍵を入手し、当該入手した公開鍵を用いて、受信したコンテンツプロバイダセキュアコンテナの署名を検証する。署名の検証に成功した後、コンテンツプロバイダセキュアコンテナから暗号化されたコンテンツを取り出し、当該取り出した暗号化されたコンテンツをサーバ 3 4 2 に保持すると共に、残りの鍵データ（暗号化されたコンテンツ鍵  $K_c$  や、暗号化された個別鍵  $K_i$ 、（図示せず））および取扱方針等を K I O S K 端末 3 3 2 に送信する。

K I O S K 端末 3 3 2 は、受信した鍵データ（暗号化されたコンテンツ鍵  $K_c$  や、暗号化された個別鍵  $K_i$ 、（図示せず））および取扱方針等を保持すると共に、当該 K I O S K 端末 3 3 2 を管理する情報提供者側で作成された価格情報を保持する。

ここで、実際に K I O S K 端末 3 3 2 において実行される購入処理を図 1 0 2 乃至図 1 0 5 に示すフローチャートを用いて説明する。ステップ S 7 8 0 において、顧客がメディア（記録メディア 3 3 3 または電子配信専用記録メディア 3 3 4）を K I O S K 端末 3 3 2 に挿入すると、ステップ S 7 8 1 において、K I O

S K端末332の上位コントローラ351は挿入されたメディアが記録メディア333（この実施の形態では例えばMD（商標））であるか否かを判断し、挿入されたメディアが記録メディア333である場合には、ステップS782に進む。

ステップS782において、上位コントローラ351は、表示手段356を介して購入可能なコンテンツ（すなわち、曲名）および価格等の情報を表示させ、この状態において、顧客が入力手段355を介して所望するコンテンツを選択指定し、代金投入口にお金を投入すると、ステップS783に進む。ステップS783において、上位コントローラ351は、代金処理部354を用いて顧客の投入したお金が請求する代金に対して不足していないか否かを判断し、不足していない場合（顧客が投入したお金が代金よりも多くても良い）には、ステップS785に進む。因みに、ステップS783において、顧客の投入したお金が請求する代金に対して不足している場合には、ステップS784に進み、顧客に対して、不足分のお金を代金投入口投入するように表示手段356を介して通知する。

ステップS785において、上位コントローラ351は、顧客が選択指定したコンテンツに対応する取扱方針、価格情報および鍵データをK I O S K端末サーバ357から読み出し、これらを暗号処理部352に送出して制御部360に購入処理を実行するように命令する。

次いで、ステップS786において、暗号処理部352の制御部360は、購入処理モジュール363において、上位コントローラ351から与えられた取扱方針および価格情報に基づいて、顧客の選択指定したコンテンツに対する、例えば、複製回数が1回に制限された（すなわち、K I O S K端末332から記録メディア333への複製）コピー管理情報（SCMS）付き複製権の購入処理を実行し、この結果、生成した課金情報を記憶モジュール361に保持する。

因みに、記録メディア333にコンテンツを記録した後、当該記録メディア333から他の記録メディア333にコンテンツが不当に複製されることを防止するため、K I O S K端末332は、コピー管理情報付き複製権の購入処理を実行

するようにしている。しかしながら、コンテンツの不当な複製を防止し得れば、回数制限付きコピー制御情報無し複製権や、本実施の形態では記録メディア 3 3 3 を MD (商標) としているが、メモリスティック (商標) 等の各種メディアや、記録媒体に応じた制限付き複製権等の購入処理を実行しても良い。

次いで、ステップ S 7 8 7 において、暗号処理部 3 5 2 の制御部 3 6 0 は、暗号／復号化モジュール 3 6 5 の復号化ユニット 3 7 0 において、上位コントローラ 3 5 1 から与えられる鍵データに含まれる暗号化された個別鍵  $K_i$  および暗号化されたコンテンツ鍵  $K_{co}$  を取り出し、当該暗号化された個別鍵  $K_i$  を記憶モジュール 3 6 1 に記憶している配送鍵  $K_d$  を用いて復号化し、得られた個別鍵  $K_i$  を用いて、暗号化されているコンテンツ鍵  $K_{co}$  を復号化する。

続いて、ステップ S 7 8 8 において、暗号処理部 3 5 2 の制御部 3 6 0 は、電子透かし挿入部 3 5 3 との間で互いの相互認証モジュール 3 6 4 および 3 8 0 を用いて相互認証を行い、一時鍵  $K_{temp}$  を共有化し、ステップ S 7 8 9 に進む。ステップ S 7 8 9 において、暗号処理部 3 5 2 の制御部 3 6 0 は、暗号／復号化モジュール 3 6 5 の暗号化ユニット 3 7 1 において、復号化されているコンテンツ鍵  $K_{co}$  を一時鍵  $K_{temp}$  を用いて暗号化する。そして、ステップ S 7 9 0 において、暗号処理部 3 5 2 の制御部 3 6 0 は、この一時鍵  $K_{temp}$  で暗号化したコンテンツ鍵  $K_{co}$  を電子透かし挿入部 3 5 3 に送出する。

ステップ S 7 9 1 において、電子透かし挿入部 3 5 3 は、鍵復号化モジュール 3 8 1 において、暗号処理部 3 5 2 から与えられた暗号化されたコンテンツ鍵  $K_{co}$  を、相互認証モジュール 3 8 0 から与えられる一時鍵  $K_{temp}$  (暗号処理部 3 5 2 と共有化した) を用いて復号化する。

次いで、ステップ S 7 9 2 において、上位コントローラ 3 5 1 は、顧客の選択指定したコンテンツの読出要求 (例えば、コンテンツの ID を含む) を通信部 3 5 0 を介してホスティングサーバ 3 3 1 に送信し、当該ホスティングサーバ 3 3 1 から顧客の選択指定した、暗号化されたコンテンツを読み出し、これを電子透かし挿入部 3 5 3 に送出する。因みに、上位コントローラ 3 5 1 は、このように

ホスティングサーバ 331 から暗号化されたコンテンツを読み出したときには、当該暗号化されたコンテンツを K I O S K 端末サーバ 357 にも保存し得るため、顧客がコンテンツを選択指定した場合には、まず、K I O S K 端末サーバ 357 に保持しているコンテンツを検索し、当該 K I O S K 端末サーバ 357 内に対応するコンテンツがない場合にホスティングサーバ 331 からコンテンツを読み出すようにしても良い。また、コンテンツの読み出しは、ステップ S 792 よりも以前のステップにおいて、実行しても良い。

ステップ S 793 において、電子透かし挿入部 353 は、復号化モジュール 382 において、上位コントローラ 351 から与えられる暗号化されたコンテンツを、復号化したコンテンツ鍵  $K_c$  を用いて復号化した後、電子透かし付加モジュール 383 において、この復号化されたコンテンツに、例えば、K I O S K 端末 332 の所有者の ID を電子透かしの形で挿入する。

因みに、コンテンツに付加する電子透かしのデータとして、K I O S K 端末 332 の所有者の ID を用いることは、記録メディア 333（または電子配信専用記録メディア 334）に記録したコンテンツが不正に複製されたときに、当該コンテンツを提供した K I O S K 端末 332 を特定するためである。

次いで、ステップ S 794 において、電子透かし挿入部 353 は、電子透かしを挿入したコンテンツをそのまま（デジタルデータの形式）記録メディア 333 に送出し、かくして、記録メディア 333 に顧客の指定したコンテンツを記録する。

続いて、ステップ S 795 において、上位コントローラ 351 は、代金処理部 354 を用いて、顧客が代金投入口に投入したお金が請求する代金よりも多いか否かを判断し、当該お金が代金に対して多い場合には、その差額を代金返却口から釣り銭として返金する。

かくして、ステップ S 796 において、顧客は、釣り銭がある場合には当該釣り銭を受け取ると共に、記録メディア 333 を受け取る。

因みに、K I O S K 端末 332 の上位コントローラ 351 は、このように顧客



がコンテンツの利用権を購入すると、この際作成した課金情報を電子配信サービスセンタ 1 に送信する。これにより、電子配信サービスセンタ 1 は、この課金情報に基づいて決済し、かくして、購入処理した利用権に応じて、K I O S K 端末 3 3 2 の保有者から、顧客の支払った代金の一部を回収する。

一方、上位コントローラ 3 5 1 は、ステップ S 8 0 0 において、顧客が K I O S K 端末 3 3 2 に電子配信専用記録メディア 3 3 4 を挿入したときには、続くステップ S 8 0 1 のメディアの判別処理により当該メディアが電子配信専用記録メディア 3 3 4 であると判別するため（すなわち、ステップ S 7 8 1 について上述したメディアの判別処理により、K I O S K 端末 3 3 2 に顧客の挿入したメディアが電子配信専用記録メディア 3 3 4 の場合）、ステップ S 8 0 2 に進む。因みに、このステップ S 8 0 1 でメディアが記録メディア 3 3 3 であると判別した場合には、ステップ S 7 8 2 以降の処理を実行する。

ステップ S 8 0 2 において、上位コントローラ 3 5 1 は、表示手段 3 5 6 を介して購入可能なコンテンツ（すなわち、曲名）および価格と共に、当該コンテンツに対して購入可能な利用権を設定し（例えば、無制限再生権、期間制限付き再生権、積算時間制限付き再生権、回数制限付き再生権、無制限複製権、回数制限付き複製権等）、当該設定した利用権の内容等の情報を表示させ、この状態において、顧客が入力手段 3 5 5 を介して所望するコンテンツを選択指定すると共に、所望する利用権内容を選択指定すると、ステップ S 8 0 3 に進む。

ステップ S 8 0 3 において、上位コントローラ 3 5 1 は、表示手段 3 5 6 を介して利用権の購入代金を後日決済とするか否かを問い合わせる。そして、顧客が入力手段 3 5 5 を介して代金をその場で支払うことを選択すると、上位コントローラ 3 5 1 は、これを受けて、表示手段 3 5 6 を介して代金投入口にお金を投入するように促し、ステップ S 8 0 4 に進む。因みに、ステップ S 8 0 4 は、ステップ S 7 8 3 について上述した処理と同様の処理を実行するため、その説明は省略する。また、ステップ S 8 0 4 から進むことのできるステップ S 8 0 5 は、ステップ S 7 8 4 について上述した処理と同様の処理を実行するため、その説明を省

略する。

次いで、ステップS 8 0 6において、上位コントローラ3 5 1は、表示手段3 5 6を介して、顧客に購入処理をK I O S K端末3 3 2で実行しても良いか否かを問い合わせる。そして、顧客が入力手段3 5 5を介して購入処理をK I O S K端末3 3 2が実行しても良いことを選択すると、上位コントローラ3 5 1は、ステップS 8 0 7に進む。

ステップS 8 0 7は、ステップS 7 8 5について上述した処理と同様の処理を実行するため、その説明を省略する。次いで、ステップS 8 0 8において、K I O S K端末3 3 2内の暗号処理部3 5 2の制御部3 6 0は、購入処理モジュール3 6 3において、上位コントローラ3 5 1から与えられた取扱方針および価格情報に基づいて、顧客の選択指定した利用権の購入処理を実行し、使用許諾条件情報および課金情報を作成し、当該課金情報を記憶モジュール3 6 1に保持した後、ステップS 8 0 9に進む。ステップS 8 0 9は、ステップS 7 8 7について上述した処理と同様の処理を実行するため、その説明を省略する。

因みに、使用許諾条件情報のデータに格納される暗号処理部のID（すなわち、この使用許諾条件情報を作成した暗号処理部のID）としては、電子配信専用記録メディア3 3 4内の暗号処理部1 2 2のIDを格納する（ただし、K I O S K端末3 3 2内の暗号処理部3 5 2のIDを格納してもかまわない。このとき、コンテンツを受け渡した電子配信専用記録メディア3 3 4内の暗号処理部1 2 2のIDをK I O S K端末サーバ3 5 7に保存しておき、後に電子配信サービスセンタ1へ送信して管理する場合がある）。

次いで、ステップS 8 1 0において、K I O S K端末3 3 2内の暗号処理部3 5 2の制御部3 6 0は、電子配信専用記録メディア3 3 4の暗号処理部1 2 2との間で互いの相互認証モジュール3 6 4および1 2 8を用いて相互認証し、一時鍵 $K_{temp}$ を共有化し、ステップS 8 1 1に進む。

ステップS 8 1 1において、K I O S K端末3 3 2内の暗号処理部3 5 2の制御部3 6 0は、暗号／復号化モジュール3 6 5の暗号化ユニット3 7 1において

、復号化したコンテンツ鍵 $K_{co}$ と、使用許諾条件情報とをそれぞれ一時鍵 $K_{temp}$ を用いて暗号化する。因みに、コンテンツ鍵 $K_{co}$ および使用許諾条件情報のうち、使用許諾条件情報はその内容が見られても、特に問題ないため、コンテンツ鍵 $K_{co}$ のみを暗号化しても良い。そして、KIOSK端末332内の暗号処理部352の制御部360は、署名生成ユニット373において、暗号化された（一時鍵 $K_{temp}$ で）コンテンツ鍵 $K_{co}$ および使用許諾条件情報（暗号化されている場合がある）全体（または別々）に対して署名を生成し、上位コントローラ351に返送する。

次いで、ステップS812において、KIOSK端末332内の上位コントローラ351は、ステップS792と同様にホスティングサーバ331またはKIOSK端末サーバ357から顧客が選択指定した、暗号化されたコンテンツを読み出す（因みに、コンテンツの読み出しタイミングは、このステップS812よりも以前のステップにおいて実行しても良い）。そして、読み出したコンテンツ、暗号化された（一時鍵 $K_{temp}$ で）コンテンツ鍵 $K_{co}$ 、使用許諾条件情報と、当該暗号化された（一時鍵 $K_{temp}$ で）コンテンツ鍵 $K_{co}$ および使用許諾条件情報に対する署名と、KIOSK端末サーバ357から読み出された取扱情報、価格情報が上位コントローラ351を介して電子配信専用記録メディア334に送信される。

ステップS813において、電子配信専用記録メディア334内の暗号処理部122の制御部124は、署名検証ユニット135において、KIOSK端末332から与えられる暗号化された（一時鍵 $K_{temp}$ で）コンテンツ鍵 $K_{co}$ 、取扱情報、価格情報および使用許諾条件情報に対する署名の検証を行い、この後、復号化ユニット132において、暗号化されているコンテンツ鍵 $K_{co}$ と、必要に応じて暗号化されている使用許諾条件情報とをそれぞれ一時鍵 $K_{temp}$ を用いて復号化する。そして、制御部124は、暗号化ユニット132において、復号化されているコンテンツ鍵 $K_{co}$ を、記憶モジュール125に保持している保存鍵 $K_{save}$ を用いて暗号化する。

そして、ステップS814において、電子配信専用記録メディア334内の暗

号処理部 122 の制御部 124 は、コンテンツ鍵  $K_{co}$  で暗号化されているコンテンツ、保存鍵  $K_{save}$  で暗号化されているコンテンツ鍵  $K_{co}$ 、取扱方針、価格情報および使用許諾条件情報を外部メモリ制御部 130 を介して外部メモリ 123 に保存する。因みに、保存鍵  $K_{save}$  で暗号化されているコンテンツ鍵  $K_{co}$  と、使用許諾条件情報は、外部メモリ制御部 130 により外部メモリ 123 内の改竄チェックされた領域に保存する。

そして、KIOSK 端末 332 内の上位コントローラ 351 は、この後ステップ S815 およびステップ S816 に順次進むものの、当該ステップ S815 およびステップ S816 は、それぞれステップ S795 およびステップ S796 について上述した処理と同様の処理を実行するため、その説明は省略する。

因みに、KIOSK 端末 332 の上位コントローラ 351 は、電子配信専用記録メディア 334 に暗号化されたコンテンツ、暗号化されたコンテンツ鍵  $K_{co}$ 、取扱方針、価格情報および使用許諾条件情報は送信するものの、課金情報は内部の記憶モジュール 361 に保持するため、当該課金情報を電子配信サービスセンタ 1 に送信する。これにより、電子配信サービスセンタ 1 は、この課金情報に基づいて決済し、かくして、購入処理した利用権に応じて、KIOSK 端末 332 の保有者から、顧客の支払った代金の一部を回収する。

ここで、ステップ S803 について上述した代金の決済において、顧客が入力手段 355 を介して利用権の購入代金を後日決済とすることを選択すると、KIOSK 端末 332 内の上位コントローラ 351 は、ステップ S820 に進む。因みに、このステップ S820 からこれに続くステップ S823 までの処理は、ステップ S807 からこれに続くステップ S810 までの処理と同様であるため、その説明は省略する。ただし、ステップ S821 において生成された課金情報は、暗号処理部 352 の記憶モジュール 361 には保存されない。

次いで、ステップ S824 において、KIOSK 端末 332 内の暗号処理部 352 の制御部 360 は、暗号／復号化モジュール 365 の暗号化ユニット 371 において、復号化したコンテンツ鍵  $K_{co}$ 、使用許諾条件情報および課金情報をそ

れぞれ一時鍵 $K_{temp}$ を用いて暗号化する。因みに、コンテンツ鍵 $K_{co}$ の以外の使用許諾条件情報および課金情報はその内容が見られても、特に問題ないため、コンテンツ鍵 $K_{co}$ のみを暗号化しても良い。そして、KIOSK端末332内の暗号処理部352の制御部360は、署名生成ユニット373において、暗号化された（一時鍵 $K_{temp}$ で）コンテンツ鍵 $K_{co}$ 、暗号化された使用許諾条件情報および暗号化された課金情報全体に対して（またはそれぞれに対して）署名を生成し、暗号化された（一時鍵 $K_{temp}$ で）コンテンツ鍵 $K_{co}$ 、暗号化された使用許諾条件情報、暗号化された課金情報および署名を上位コントローラ351に送信する。

次いで、ステップS825において、KIOSK端末332内の上位コントローラ351は、ステップS792と同様にホスティングサーバ331またはKIOSK端末サーバ357から顧客が選択指定した、暗号化されたコンテンツを読み出す（因みに、コンテンツの読み出しタイミングは、このステップS812よりも以前のステップにおいて実行しても良い）。

そして、暗号化されたコンテンツ、暗号化された（一時鍵 $K_{temp}$ で）コンテンツ鍵 $K_{co}$ 、取扱情報、価格情報、暗号化された使用許諾条件情報および暗号化された課金情報と、当該暗号化された（一時鍵 $K_{temp}$ で）コンテンツ鍵 $K_{co}$ 、暗号化された使用許諾条件情報および暗号化された課金情報全体に対して（またはそれぞれに対して）生成された署名とを上位コントローラ351を介して電子配信専用記録メディア334に送信する。また、取扱方針および価格情報は必要に応じてKIOSK端末332から電子配信専用記録メディア334に送信しても良い。

ステップS826において、電子配信専用記録メディア334内の外部メモリ制御部130は、暗号化されたコンテンツを外部メモリ123に保存する。因みに、外部メモリ制御部130は、取扱情報および価格情報を必要に応じて外部メモリ123に保存する。

次いで、ステップS827において、電子配信専用記録メディア334内の暗号処理部122の制御部124は、署名検証ユニット135において、KIOSK端末332から与えられる暗号化された（一時鍵 $K_{temp}$ で）コンテンツ鍵 $K_{co}$ 、

暗号化された使用許諾条件情報および暗号化された課金情報に対する署名の検証を行い、復号化ユニット132において、暗号化されているコンテンツ鍵 $K_c$ 、暗号化されている使用許諾条件情報および暗号化されている課金情報をそれぞれ一時鍵 $K_{temp}$ を用いて復号化する（使用許諾条件情報および課金情報が暗号化されていない場合にはその必要はない）。そして、制御部124は、暗号化ユニット132において、復号化されているコンテンツ鍵 $K_c$ を、記憶モジュール125に保存している保存鍵 $K_{save}$ を用いて暗号化する。

そして、ステップS828において、電子配信専用記録メディア334内の暗号処理部122の制御部124は、課金情報を記憶モジュール125に保存する。ついで、ステップS829において、電子配信専用記録メディア334内の暗号処理部122の制御部124は、暗号化されているコンテンツ鍵 $K_c$ および使用許諾条件情報を外部メモリ制御部130を介して外部メモリ123に保存する。因みに、コンテンツ鍵 $K_c$ および使用許諾条件情報は、外部メモリ制御部130により外部メモリ123内の改竄チェックされた領域に保存する。

ところで、このように後日決済により電子配信専用記録メディア334にコンテンツを記録し、当該電子配信専用記録メディア334内に課金情報も保存すると、この後、電子配信専用記録メディア334を、電子配信サービスセンタ1に接続された機器に挿入するまでの間は当該電子配信サービスセンタ1がこの電子配信専用記録メディア334から課金情報を回収することができない。このため、電子配信専用記録メディア334を、電子配信サービスセンタ1に接続されていない機器に挿入して、代金未払いのまま、コンテンツが不当に利用される可能性がある。

従って、かかる電子配信専用記録メディア334においては、コンテンツを記録した後、当該電子配信専用記録メディア334内の暗号処理部122の制御部124が所定のタイミングで記憶モジュール125の課金情報を検索し、未回収の課金情報が保存されている場合には、当該課金情報が回収されるまでの間、対応するコンテンツの利用権に回数や、時間等の制限を加えて、当該制限内におい

てのみコンテンツを利用し得るようにする。これによりコンテンツの不当な利用を防止する。

また、かかる購入処理においては、K I O S K 端末 3 3 2 内に当該購入処理において生成した課金情報や、使用許諾条件情報、これらの作成に用いた取扱方針等が残らないため、電子配信サービスセンタ 1 は、この際、電子配信専用記録メディア 3 3 4 を所有する顧客から代金を回収し、当該回収した代金から購入された利用権に応じて、この代金の一部を K I O S K 端末 3 3 2 の保有者に配当する。

また、ステップ S 8 0 6 について上述した処理において、顧客が入力手段 3 5 5 を介して電子配信専用記録メディア 3 3 4 により購入処理を実行するように選択した場合には、ステップ S 8 4 0 に進み、K I O S K 端末 3 3 2 内の上位コントローラ 3 5 1 は、ステップ S 7 9 2 と同様に顧客の選択指定したコンテンツをホスティングサーバ 3 3 1 または K I O S K 端末サーバ 3 5 7 から読み出すと共に、当該 K I O S K 端末サーバ 3 5 7 から対応する鍵データ、取扱方針および価格情報を読み出し、これらを電子配信専用記録メディア 3 3 4 に送信する。

因みに、K I O S K 端末 3 3 2 においては、電子配信専用記録メディア 3 3 4 と相互認証した後、一時鍵  $K_{temp}$  を共有化し、コンテンツ（コンテンツ鍵  $K_c$  で暗号化されている）、鍵データ、取扱方針、価格情報を当該一時鍵  $K_{temp}$  で必要に応じて暗号化し、それらのデータ全体または一部に署名を付加しても良い。

ステップ S 8 4 1 において、電子配信専用記録メディア 3 3 4 内の暗号処理部 1 2 2 の制御部 1 2 4 は、コンテンツ（コンテンツ鍵  $K_c$  で暗号化されている）を外部メモリ制御部 1 3 0 を介して外部メモリ 1 2 3 に保存すると共に、必要に応じて取扱方針および価格情報を外部メモリ制御部 1 3 0 を介して外部メモリ 1 2 3 に保存する。

次いで、ステップ S 8 4 2 において、電子配信専用記録メディア 3 3 4 内の暗号処理部 1 2 2 の制御部 1 2 4 は、購入処理モジュール 1 2 7 において、購入処理を実行し、取扱方針および価格情報に基づいて、使用許諾条件情報および課金

情報を作成する。因みに、購入処理の手順は、図 6 7 について上述したステップ S 1 6 3 からステップ S 1 7 0 までと同様であるため、その詳細な説明は省略する。

続いて、ステップ S 8 4 3 において、電子配信専用記録メディア 3 3 4 内の暗号処理部 1 2 2 の制御部 1 2 4 は、復号化ユニット 1 3 1 において、鍵データに含まれる暗号化されている個別鍵  $K_i$  を、記憶モジュール 1 2 5 に保持している配送鍵  $K_d$  を用いて復号化した後、当該鍵データに含まれる暗号化されているコンテンツ鍵  $K_c$  を、復号化した個別鍵  $K_i$  を用いて復号化する。そして、制御部 1 2 4 は、暗号化ユニット 1 3 2 において、復号化されているコンテンツ鍵  $K_c$  を、記憶モジュール 1 2 5 に保持している保存鍵  $K_{save}$  を用いて暗号化する。

次いで、ステップ S 8 4 4 において、電子配信専用記録メディア 3 3 4 内の暗号処理部 1 2 2 の制御部 1 2 4 は、K I O S K 端末 3 3 2 内の暗号処理部 3 5 2 との間で互いの相互認証モジュール 1 2 8 および 3 6 4 を用いて相互認証して一時鍵  $K_{temp}$  を共有化する。

そして、ステップ S 8 4 5 において、電子配信専用記録メディア 3 3 4 内の暗号処理部 1 2 2 の制御部 1 2 4 は、暗号化ユニット 1 3 2 において、課金情報を一時鍵  $K_{temp}$  を用いて暗号化し、署名生成ユニット 1 3 4 において、当該課金情報に署名を付加した後、この暗号化した課金情報および署名を通信部 1 2 1 を介して K I O S K 端末 3 3 2 に送信する。因みに、課金情報には改竄されないように署名を付加するものの、特に暗号化せずに電子配信専用記録メディア 3 3 4 に送信しても良い。そして、課金情報を暗号化しない場合には、電子配信専用記録メディア 3 3 4 と、K I O S K 端末 3 3 2 との間で一時鍵  $K_{temp}$  を共有化しなくても良い。

ステップ S 8 4 6 において、K I O S K 端末 3 3 2 内の上位コントローラ 3 5 1 は、電子配信専用記録メディア 3 3 4 から送信された課金情報および署名を暗号処理部 3 5 2 に送出する。これにより、ステップ S 8 4 7 において、K I O S K 端末 3 3 2 内の暗号処理部 3 5 2 の署名検証ユニット 3 7 4 は、課金情報に対



する署名を検証し、当該署名の検証に成功した後、復号化ユニット370において、課金情報を一時鍵 $K_{temp}$ を用いて復号化して記憶モジュール361に保存する。

そして、ステップS848において、KIOSK端末332内の暗号処理部352の制御部360は、課金処理が完了したことを示す課金処理完了通知を生成し、署名生成ユニット373において、この課金処理完了通知に署名を付加し、当該署名を付加した課金処理完了通知を上位コントローラ351に送出すると共に、当該上位コントローラ351を介して電子配信専用記録メディア334に送信する。これにより、上位コントローラ351は、課金処理完了通知に基づいて、特に署名を検証せずに、単に課金処理が終了したか否かを判断する。また、電子配信専用記録メディア334内の暗号処理部122の制御部124は、署名検証ユニット135において、課金処理完了通知の署名を検証し、かくして、課金処理の終了を認識する。

そして、ステップS849において、電子配信専用記録メディア334内の暗号処理部122の制御部124は、保存鍵 $K_{save}$ で暗号化しているコンテンツ鍵 $K_c$ および使用許諾条件情報を外部メモリ制御部130を介して外部メモリ123の改竄チェックされた領域に保存する。

次いで、KIOSK端末332は、ステップS850およびステップS851の処理を順次実行するものの、当該処理はステップS815およびステップS816において実行した処理と同様であるため、その説明は省略する。

このように、電子配信専用記録メディア334において購入処理したときには、KIOSK端末332に課金情報を保持し、当該KIOSK端末332から電子配信サービスセンタ1にこの課金情報を送信する。

因みに、ステップS803において、顧客が利用権の購入代金を後日決済とすることを選択した場合、図106に示すステップS860において、電子配信専用記録メディア334の上位コントローラ351は、コンテンツプロバイダ2から送信されたコンテンツプロバイダセキュアコンテナの状態で、暗号化されてい

るコンテンツ、鍵データ、取扱方針および価格情報を電子配信専用記録メディア 334 に送信しても良い。そして、このように K I O S K 端末 332 から電子配信専用記録メディア 334 にコンテンツプロバイダセキュアコンテナの状態データを送信する場合には、コンテンツプロバイダ 2 において当該コンテンツプロバイダセキュアコンテナに既に署名が付加されていることにより、K I O S K 端末 332 は特に署名を付加せずに電子配信専用記録メディア 334 に送信する。

また、ステップ S 803 において、顧客が利用権の購入代金を後日決済とすることを選択した場合、K I O S K 端末 332 においては、図 107 に示すフローチャートを用いて説明する購入処理を実行するようにしても良い。すなわち、ステップ S 870 において、K I O S K 端末 332 内の上位コントローラ 351 は、暗号処理部 352 の制御部 360 に購入処理を実行するように命令する。因みに、このステップ S 870 の処理は、ステップ S 785 の処理と同様であるため、その詳細な説明は省略する。

次いで、ステップ S 871 において、K I O S K 端末 332 内の暗号処理部 352 の制御部 360 は、復号化ユニット 370 において、暗号化されている個別鍵  $K_i$  を、記憶モジュール 361 に保持している配送鍵  $K_d$  を用いて復号化した後、暗号化されているコンテンツ鍵  $K_c$  を、この復号化した個別鍵  $K_i$  を用いて復号化し、ステップ S 872 に進む。因みに、ステップ S 872 の処理は、ステップ S 810 について上述した処理と同様であるため、その説明は省略する。

続いて、ステップ S 873 において、K I O S K 端末 332 内の暗号処理部 352 の制御部 360 は、暗号化ユニット 371 において、復号化されているコンテンツ鍵  $K_c$  を一時鍵  $K_{temp}$  を用いて暗号化し、必要に応じて署名検証ユニット 373 において、暗号化されている（一時鍵  $K_{temp}$  で）コンテンツ鍵  $K_c$  に対して署名を生成し、ステップ S 874 に進み、当該ステップ S 874 において、署名生成ユニット 373 において、暗号化されているコンテンツ、暗号化されている（一時鍵  $K_{temp}$  で）コンテンツ鍵  $K_c$  およびその署名、取扱方針および価格情報を上位コントローラ 351 を介して電子配信専用記録メディア 334 に送信する。

ステップS 8 7 5において、電子配信専用記録メディア3 3 4内の暗号処理部1 2 2の制御部1 2 4は、署名検証ユニット1 3 5において、暗号化されている（一時鍵 $K_{temp}$ で）コンテンツ鍵 $K_c$ の署名を検証した後、復号化ユニット1 3 1において、暗号化されているコンテンツ鍵 $K_c$ を、一時鍵 $K_{temp}$ を用いて復号化する。そして、制御部1 2 4は、暗号化ユニット1 3 2において、復号化されているコンテンツ鍵 $K_c$ を、記憶モジュール1 2 5に保持している保存鍵 $K_{save}$ を用いて暗号化する。

そして、ステップS 8 7 6において、電子配信専用記録メディア3 3 4内の暗号処理部1 2 2の制御部1 2 4は、購入処理モジュール1 2 7において、購入処理を実行し、取扱方針および価格情報に基づいて、使用許諾条件情報および課金情報を作成した後、ステップS 8 7 7に進んで、当該課金情報を記憶モジュール1 2 5に保存する。

次いで、ステップS 8 7 8において、電子配信専用記録メディア3 3 4内の暗号処理部1 2 2の制御部1 2 4は、暗号化されているコンテンツ、取扱方針、価格情報を外部メモリ制御部1 3 0を介して外部メモリ1 2 3に保存し、続いて、ステップS 8 7 9において、暗号化されたコンテンツ鍵 $K_c$ および使用許諾条件情報を外部メモリ制御部1 3 0を介して外部メモリ1 2 3の改竄チェックされた領域に保存する。因みに、ステップS 8 7 8において、制御部1 2 4は、使用許諾条件情報に取扱方針および価格情報に含まれる各種情報を盛り込むため、当該取扱方針および価格情報を必要に応じて外部メモリ1 2 3に保存すれば良い。

このように、K I O S K端末3 3 2においては、記録メディア3 3 3および電子配信専用記録メディア3 3 4に対してコンテンツの利用権に対する購入処理を実行して、当該記録メディア3 3 3および電子配信専用記録メディア3 3 4にコンテンツを記録し得る。

因みに、記録メディア3 3 3を所持する顧客は、当該記録メディア3 3 3に復号化したコンテンツが記録されることにより、当該記録メディア3 3 3に応じて、伸張部および暗号処理部を持たず、また、サービスプロバイダ3や電子配信サ

ービスセンタ 1 に接続する必要のない再生装置を用いてコンテンツを容易に利用し得る。

また、電子配信専用記録メディア 3 3 4 を所持する顧客は、図 1 5 について上述したホームサーバ 5 1 のように、伸張部（または、これに加えて暗号処理部）が設けられた再生装置を用いなければ、コンテンツを利用することはできないが、当該再生装置が電子配信サービスセンタ 1 や、サービスプロバイダ 3 に直接および間接的のいずれにおいても接続されている必要はないため、ユーザホームネットワーク 5 を構築するために用いる再生装置等の機器でも、コンテンツを利用し得る。

以上の構成において、この電子音楽配信システム 1 0 では、K I O S K 端末 3 3 2 に記録メディア 3 3 3 が挿入された場合、当該 K I O S K 端末 3 3 2 において、購入処理を実行するようにして復号化したコンテンツに電子透かしのデータを挿入して記録メディア 3 3 3 に記録するようにした。

また、K I O S K 端末 3 3 2 に電子配信専用記録メディア 3 3 4 が挿入された場合には、当該 K I O S K 端末 3 3 2 または電子配信専用記録メディア 3 3 4 のいずれかにおいて購入処理を実行し、当該電子配信専用記録メディア 3 3 4 に暗号化されているコンテンツおよびコンテンツ鍵 K<sub>c</sub>。並びに使用許諾条件情報を記録するようにした。

従って、かかる電子音楽配信システム 1 0 では、顧客がサービスプロバイダ 3 や、電子配信サービスセンタ 1 に接続されたユーザホームネットワーク 5 を構築する機器等を所有していなくても、簡易小売店に設置された K I O S K 端末 3 3 2 により当該顧客が所持する記録メディア 3 3 3 および電子配信専用記録メディア 3 3 4 にそれぞれコンテンツを安全性を確保して記録することができる。

すなわち、記録メディア 3 3 3 には、コンテンツを S C M S 等のコピー制御信号を付加した状態で記憶したり、電子透かしによりコピー管理（コピー管理情報付き複製権）して記録するため、当該コンテンツが不正に複写されることを防止することができる。因みに、電子透かし信号には、コピー制御信号（コピー可／

付加を制御する信号)、再生制御信号(再生可/付加を制御する信号)、何らかの機器のID(KIOSK端末のIDや電子配信専用記録メディア334のID)等が考えられ、そのいずれかを1つまたは複数埋め込むようにしても良い。

また、電子配信専用記録メディア334には、購入処理において選定した利用権(無制限、回数制限、時間制限等)や、購入処理を後日決済にした場合に課金情報が回収されるまでの間、利用権に加えられる制限を使用許諾条件情報によって管理するため、この場合にもコンテンツが不正に利用されることを防止することができる。

以上の構成によれば、KIOSK端末332により記録メディア333および電子配信専用記録メディア334にコンテンツを記録するようにしたことにより、ユーザホームネットワーク5を構築する機器を所有していないユーザに対しても、当該記録メディア333および電子配信専用記録メディア334にコンテンツを安全性を確保して記録するようにして容易に提供し得る。

また、KIOSK端末332を所有する情報提供者(図1ではサービスプロバイダ3)が価格情報を提供しているため、図103、図105および図106のいずれの系においても、コンテンツ提供手数料が情報提供者に分配されるため、直接お金を回収する図101、図102および図104と実質的に差がない。

#### (11) KIOSK端末332におけるアルバム化コンテンツの提供

かかる構成に加えて情報提供装置330の場合、KIOSK端末332のKIOSK端末サーバ357には、当該KIOSK端末332を所有する情報提供者が、ホスティングサーバ331に保存するコンテンツに対して生成した、アーティスト、当該アーティストの性別、曲の種別(演歌や、ロックンロール等)、曲のイメージする季節、場所(海や山等)および時間帯(夕暮れ時、朝等)等のキーワード情報が保存される。因みに、別の例としては、コンテンツプロバイダ2がこのキーワード情報を生成し、当該生成したキーワード情報をホスティングサーバ331内のコンテンツサーバであるサーバ342またはKIOSK端末サーバ357に保存する場合もある。

また、K I O S K 端末 3 3 2 の K I O S K 端末サーバ 3 5 7 には、情報提供者が生成した、コンテンツ毎またはキーワード毎に異なる（無理に代えなくても良い）各種提供情報（例えば、コマーシャル、コンテンツ情報等）も保存している。因みに、コンテンツプロバイダ 2 が当該提供情報を生成し、ホスティングサーバ 3 3 1 のサーバ 3 4 2 または K I O S K 端末 3 3 2 の K I O S K 端末サーバ 3 5 7 に保存しておくようにしても良いし、コンテンツプロバイダ 2 が生成した、または情報提供者から受信した提供情報をコンテンツにリンクさせて 1 つのコンテンツとしてまとめても良い（すなわち、音楽（コンテンツ）の先頭、中間、最後等に提供情報を埋め込んで、あたかも 1 つの曲とし、当該音楽と提供情報とが簡単には分離できないようにする）。

K I O S K 端末 3 3 2 の選定手段および格納手段である上位コントローラ 3 5 1 は、キーワード情報に基づいて、ホスティングサーバ 3 3 1 のサーバ 3 4 2 に保存している複数のコンテンツをカテゴリ分けしたデータテーブルを作成し、当該作成したデータテーブルを K I O S K 端末サーバ 3 5 7 に保存する。因みに、データテーブルには、カテゴリ毎に対応するコンテンツの I D を登録する。また、このデータテーブルをホスティングサーバ 3 3 1 の制御部 3 4 1 が生成し、当該データテーブルをサーバ 3 4 2 または K I O S K 端末サーバ 3 5 7 に保存するようにしても良い。さらに、データテーブルをサーバ 3 4 2 に保存している場合、ホスティングサーバ 3 3 1 の制御部 3 4 1 は、コンテンツに対するキーワード情報を通信部 3 4 0 を介して K I O S K 端末 3 3 2 に送信し、かくして、K I O S K 端末 3 3 2 内において、上位コントローラ 3 5 1 によりこのキーワード情報を K I O S K 端末サーバ 3 5 7 に保存する。

そして、K I O S K 端末 3 3 2 においては、顧客が電子配信専用記録メディア 3 3 4 を挿入した場合、上位コントローラ 3 5 1 が K I O S K 端末サーバ 3 5 7 から購入処理可能なコンテンツに対するキーワードを読み出し、当該キーワードを表示手段 3 5 6 を介して顧客に通知する。因みに、上位コントローラ 3 5 1 は、このとき、K I O S K 端末サーバ 3 5 7 から読み出した購入処理可能なコンテ

ンツに対するキーワードをコンテンツに対する曲名や価格の情報と共に表示手段 3 5 6 を介して顧客に通知しても良い。

顧客が入力手段 3 5 5 を介して、例えば、好みのコンテンツに対応するキーワード（キーワードの数は複数でも良い）と、購入処理したいコンテンツ数を選択指定すると、その入力データは上位コントローラ 3 5 1 へ信号として送信され、これを受信した上位コントローラ 3 5 1 は、顧客の指定したコンテンツ数に基づき、自己の保持する図示せぬ乱数発生プログラムにより乱数を発生し、または暗号処理部 3 5 2 の制御部 3 6 0 を制御することにより、乱数発生手段である乱数発生ユニット 3 7 2 により乱数を発生させる。因みに、上位コントローラ 3 5 1 は、これらのキーワード、乱数を通信部 3 5 0 を介してホスティングサーバ 3 3 1 に送信する場合がある。また、乱数はコンテンツをランダムに選定するために使用されるため、無理に乱数を発生させずに、キーワードのカテゴリに属するコンテンツ全てを購入処理したり、キーワードのカテゴリに属するコンテンツを、データテーブルに現れる順番に購入処理するようにしても良い。

上位コントローラ 3 5 1 は、先ほど生成した乱数データと、入力手段 3 5 5 を介して入力されたキーワードに基づいて、K I O S K 端末サーバ 3 5 7 内のデータテーブルを検索する。そして、上位コントローラ 3 5 1 は、キーワードに対応するカテゴリに属する複数のコンテンツの I D から、当該乱数データに基づき、顧客の指定した数のコンテンツの I D を任意に選定し、当該選定したコンテンツの I D に対応するコンテンツをホスティングサーバ 3 3 1 から読み出す。

また、別の例としては、ホスティングサーバ 3 3 1 の制御部 3 4 1 が、K I O S K 端末 3 3 2 から送信された乱数のデータと、キーワードに基づき、サーバ 3 4 2 内のデータテーブルを検索することにより、当該キーワードに対応するカテゴリに属する複数のコンテンツの I D から、当該乱数のデータに基づき、顧客の指定した数のコンテンツの I D を任意に選定し、当該選定したコンテンツの I D に対応するコンテンツをサーバ 3 4 2 から読み出すと共に、これら読み出した各コンテンツを通信部 3 4 0 を介して K I O S K 端末 3 3 2 に送信する。

これにより、K I O S K 端末 3 3 2 は、ホスティングサーバ 3 3 1 から送信された複数コンテンツに対して図 1 0 3 乃至図 1 0 5 および図 1 0 6 について上述した購入処理を実行し、これら各コンテンツを電子配信専用記録メディア 3 3 4 において、記録手段である外部メモリ制御部 1 3 0 を介して記録媒体である外部メモリ 1 2 3 に一括して記録する。かくして、K I O S K 端末 3 3 2 は、電子配信専用記録メディア 3 3 4 において、顧客が好むカテゴリに属する複数の曲を一括して記録して容易にアルバム化し得る。

また、K I O S K 端末 3 3 2 における購入処理の際に、前述した提供情報とコンテンツ（あるいは、前述したように、提供情報とコンテンツが 1 つのコンテンツのように振る舞う場合がある）を、電子配信専用記録メディア 3 3 4 の外部メモリ制御部 1 3 0 を介して外部メモリ 1 2 3 に一括して記録する。再生時には、これら提供情報を顧客に聴かせるために、コンテンツの再生順序を規定できるようにし、例えば、使用許諾条件情報に制約条項を付加しても良い。そして、コンテンツの購入処理の際には、顧客が提供情報を付加する、または付加しないを選択できるようにし、提供情報を付加した際には、その代償として、購入価格を引き下げてもらう、または無料にしてもらえるようにする。かくして、顧客は、通常より安価にコンテンツの利用権を取得でき、このときにも、コンテンツプロバイダ 2 およびサービスプロバイダ 3（本実施の形態では、K I O S K 端末 3 3 2 の所有者）は、電子配信サービスセンタ 1 を介して提供情報料（いわゆる、コミーシャル料）から利益を得る。

また、K I O S K 端末 3 3 2 においては、電子配信専用記録メディア 3 3 4 に複数のコンテンツをアルバム化して記録する場合、暗号処理部 3 5 2 の制御部 3 6 0 が、これらコンテンツに対する利用権として、例えば、1 回のみ再生し得る回数制限付き再生権を選択する。さらに、K I O S K 端末 3 3 2 内の暗号処理部 3 5 2 の制御部 3 6 0、または電子配信専用記録メディア 3 3 4 内の暗号処理部 1 2 2 の制御部 1 2 4 は、使用許諾条件情報を作成する際に、当該使用許諾条件情報に格納されるサービスプロバイダ 3 の I D として、コンテンツが K I O S K



端末 3 3 2 で記録されたことがわかるような ID を格納する。例えば、サービスプロバイダ 3 の ID が 6 4 ビットである場合、上位 1 6 ビットをグループ番号、下位 4 8 ビットをシリアル番号とし、単一情報提供者が保持する K I O S K 端末 3 3 2 に割り当てる ID としては、グループ番号が全て同一で、各機器毎に下位 4 8 ビットのシリアル番号が全て異なるように割り当てる。そして、電子配信専用記録メディア 3 3 4 に記録したコンテンツが K I O S K 端末 3 3 2 で記録されたものであるか否かを判別するには、使用許諾条件情報に含まれるサービスプロバイダの ID のグループ番号により判別するようにする（すなわち、情報提供者毎にグループ番号を割り当てるようにする）。

そして、K I O S K 端末 3 3 2 においては、顧客が再び電子配信専用記録メディア 3 3 4 を挿入し、複数のコンテンツをアルバム化して記録するように要求した場合には、暗号処理部 3 5 2 の制御部 3 6 0 が電子配信専用記録メディア 3 3 4 から使用許諾条件情報を取り出し、当該使用許諾条件情報に基づいて、K I O S K 端末 3 3 2 で記録され、かつ既に再生されたコンテンツを検索する。

これにより、K I O S K 端末 3 3 2 においては、電子配信専用記録メディア 3 3 4 において、同一情報提供者の K I O S K 端末 3 3 2 により記録されたコンテンツであるものの、1 度も再生されていないコンテンツや、当該同一情報提供者の K I O S K 端末 3 3 2 とは異なる他の情報提供者の K I O S K 端末により記録されたコンテンツを削除することなく、当該情報提供者の K I O S K 端末 3 3 2 で記録され、かつ既に再生されたコンテンツのみを削除（上書き）するようにして新たなコンテンツを記録し得る。

以上の構成において、この電子音楽配信システム 1 0 では、K I O S K 端末 3 3 2 の上位コントローラ 3 5 1 により、ホスティングサーバ 3 3 1 のサーバ 3 4 2 に保存している複数のコンテンツをカテゴリ分けするデータテーブルを作成し、当該データテーブルを K I O S K 端末サーバ 3 5 7 に保存する。

そして、K I O S K 端末 3 3 2 に電子配信専用記録メディア 3 3 4 を挿入した顧客が自分の好みを表すキーワードと、まとめて購入するコンテンツの数と、必

要に応じて提供情報（コマーシャル等）を挿入する／しないを指定すると、当該 K I O S K 端末 3 3 2 は、指定されたコンテンツ数に基づいて乱数のデータを生成し、データテーブルから、指定されたキーワードのカテゴリに属する多数のコンテンツの I D を特定すると共に、当該特定したコンテンツの I D から乱数のデータに基づいて、指定された数のコンテンツの I D を任意に選定し、当該選定したコンテンツの I D に対応するコンテンツをホスティングサーバ 3 3 1 から読み出し、電子配信専用記録メディア 3 3 4 に任意に選定した複数のコンテンツおよび必要に応じて提供情報（コマーシャル等）を一括して記録する。

従って、電子配信専用記録メディア 3 3 4 に顧客の好みに応じたカテゴリに属する複数のコンテンツ（曲）を一括して記録して容易にアルバム化することができる。また、コンテンツの選定に乱数を用いるため、顧客は、電子配信専用記録メディア 3 3 4 にコンテンツを記録しなとしても、比較的高い確立で異なるコンテンツを聴くことができ、いずれの曲が記録されているかをわからないようにすることもできるため、顧客に曲を聴く楽しみを提供することができる。

さらに、電子配信専用記録メディア 3 3 4 内において、コンテンツの再生回数および当該コンテンツの記録に用いた機器を管理するため、K I O S K 端末 3 3 2 において、電子配信専用記録メディア 3 3 4 にコンテンツを記録しなす場合には、K I O S K 端末 3 3 2 で記録したものの、1 度も再生していないコンテンツや、K I O S K 端末 3 3 2 とは異なる機器で記録したコンテンツを誤って削除すること防止することができる。

以上の構成によれば、情報提供装置 3 3 0 において、K I O S K 端末 3 3 2 により、ホスティングサーバ 3 3 1 に保存している多数のコンテンツを所定のキーワードに基づいてカテゴリ分けして管理し、当該 K I O S K 端末 3 3 2 を利用する顧客が自分の好みを表すキーワードと、所望するコンテンツ数とを指定すると、当該キーワードが示すカテゴリに属する多数のコンテンツのなかから、顧客が指定した数分のコンテンツを任意に選定し、当該選定したコンテンツをホスティングサーバ 3 3 1 から読み出して電子配信専用記録メディア 3 3 4 に記録するよ

うにしたことにより、電子配信専用記録メディア 334 に、顧客の好みに応じたカテゴリに属する複数のコンテンツを一括して記録することができ、かくして好みに応じた複数のコンテンツを容易に記録し得る。

また、提供情報をコンテンツと一括して保存することにより、顧客はより安価にコンテンツの利用権を入手することができる。

なお、電子音楽配信システム 10 においては、情報記録装置である情報提供装置 330 をホスティングサーバ 331 と、KIOSK 端末 332 とを専用のケーブルまたは衛星通信等で接続して構成するようにしたが、KIOSK 端末 332 の中にホスティングサーバ 331 を一体化して設けるようにしたり、またはホスティングサーバ 331 をコンテンツプロバイダ 2 の内部に設けるようにして構成しても良い。

また、記録メディア 333 として用いるメディアは、SCMS 対応のメディアのように、複製制限を加えることができれば、MD（商標）以外の種々のメディアを適用し得る。

さらに、KIOSK 端末 332 を簡易小売店に設置するようにしたが、当該 KIOSK 端末 332 は大型店舗内や、公共施設内等のように、種々の場所に設置し得る。

さらに、購入できるコンテンツの利用権としては、1 回のみ再生し得る回数権だけではなく、期間限定された利用権も考えられ、KIOSK 端末 332 で再度購入処理する際には、すでに有効期限が切れているコンテンツを削除することもできる。

さらに、コンテンツに提供情報を付加する／しないを顧客に選択させることもできるが、コンテンツに応じて、または全てのコンテンツに対し、強制的に提供情報を付加させるようにしても良い。

#### (12) コンテンツの購入禁止処理

ここで、リスト送信装置である電子配信サービスセンタ 1（図 2）には、リスト作成手段である購入禁止リスト作成部（図 2 では図示せず）が設けられ、当該

購入禁止リスト作成部は、図 108 に示すコンテンツの購入禁止リストを作成する。コンテンツの購入禁止リストには、購入禁止対象のコンテンツの ID と、利用中止対象のコンテンツプロバイダの ID と、利用中止対象のサービスプロバイダの ID とが格納され、当該リスト全体に対しては電子配信サービスセンタ 1 の電子署名が付加されている。

コンテンツの購入禁止リストにおいて、購入禁止対象コンテンツの ID は、データに欠陥（誤り）が生じたり、またはコンテンツの提供者（コンテンツプロバイダ 2 およびサービスプロバイダ 3）側から何らかの理由で提供が中止される等して購入禁止対象となったコンテンツを示す。また、利用中止対象のコンテンツプロバイダの ID およびサービスプロバイダの ID は、購入禁止対象のコンテンツを不当に配信してコンテンツの販売権利が剥奪されたり、または倒産する等してコンテンツの配信ができなくなる等して、コンテンツの購入に利用することのできなくなったコンテンツプロバイダ 2 や、サービスプロバイダ 3 を示す。

そして、電子配信サービスセンタ 1 は、図示しない所定の送信手段を介して当該電子配信サービスセンタ 1 にオンライン接続されているユーザホームネットワーク 5 内の機器（本実施の形態では、オンライン機器であるホームサーバ 51）にコンテンツの購入禁止リストを送信する。

ホームサーバ 51 は、電子配信サービスセンタ 1 から送信されたコンテンツの購入禁止リストを通信部 61 によって受信し、上位コントローラ 62 がこの購入禁止リストを暗号処理部 65 に送出する。暗号処理部 65 は、署名検証ユニット 115 において、この購入禁止リストに付加されている電子署名を検証した後、当該購入禁止リストが改竄されていなければ、これを上位コントローラ 62 を介して、例えば、リスト保持手段である大容量記憶部 68 に保存する。因みに、ホームサーバ 51 では、電子配信サービスセンタ 1 から送信された購入禁止リストを、これに付加されている署名を検証せずに大容量記憶部 68 に保存し、購入処理等で当該購入禁止リストを使用する際に、これに付加されている署名を検証するようにしても良い。

そして、上位コントローラ 6 2 は、コンテンツプロバイダ 2 からサービスプロバイダ 3 を介してコンテンツプロバイダセキュアコンテナおよびサービスプロバイダセキュアコンテナが送信されると、例えば、コンテンツプロバイダセキュアコンテナに含まれる取扱方針またはサービスプロバイダセキュアコンテナに含まれる価格情報を暗号処理部 6 5 に送出すると共に、大容量記憶部 6 8 からコンテンツの購入禁止リストを読み出して暗号処理部 6 5 に送出する。

暗号処理部 6 5 の取込み中止処理手段である制御部 9 1 は、取扱方針または価格情報に含まれるコンテンツの提供者を示すコンテンツプロバイダの ID またはサービスプロバイダの ID、また、提供されるコンテンツの ID を用いて、コンテンツの購入禁止リスト内の情報を検索する。そして、制御部 9 1 は、この取扱方針または価格情報に含まれるコンテンツプロバイダの ID、サービスプロバイダの ID、コンテンツの ID が、コンテンツの購入禁止リスト内に存在する場合には、コンテンツの購入を行わないようにし、当該取扱方針または価格情報に含まれるコンテンツプロバイダの ID、サービスプロバイダの ID、コンテンツの ID が購入禁止リスト内に存在しない場合のみコンテンツに対する購入処理を実行する。

このように、ホームサーバ 5 1 は、購入禁止対象のコンテンツが誤って送信された場合でも、当該コンテンツを購入することを防止し得ると共に、利用中止対象のコンテンツプロバイダ 2 や、サービスプロバイダ 3 から送信されるコンテンツを購入することも防止し得る。因みに、ホームサーバ 5 1 においては、コンテンツの購入禁止リストを受信した際に、当該購入禁止リストの電子署名を検証することにより、電子配信サービスセンタ 1 において作成された正規の購入禁止リストに基づいてコンテンツの購入を禁止し得る。

また、電子配信サービスセンタ 1 においては、コンテンツの購入禁止リストに登録したコンテンツ以外に新たなコンテンツが購入禁止対象となったり、当該購入禁止リストに登録したコンテンツプロバイダ 2、サービスプロバイダ 3 以外に新たなコンテンツプロバイダ 2、サービスプロバイダ 3 が利用中止対象となる毎

に当該コンテンツの購入禁止リストを更新し、当該更新した購入禁止リストをホームサーバ51に送信する。

これにより、ホームサーバ51は、当該電子配信サービスセンタ1から購入禁止リストが送信される毎に、大容量記憶部68内の購入禁止リストを更新する。因みに、電子配信サービスセンタ1は、購入禁止リストを更新した場合、当該購入禁止リストにその更新の日付（更新日付）や、番号（シリアル番号）等を付加することにより、購入禁止リストの受信側が当該購入禁止リストが新しく更新されたものであるかを識別させ得るようになされている。

ここで、ユーザホームネットワーク5には、電子配信サービスセンタ1にオンライン接続されていない据置機器、携帯機器および電子配信専用記録メディア等（以下、これらをまとめてオフライン機器と呼ぶ）が設けられており、ホームサーバ51は、オフライン機器が接続されたときに当該オフライン機器にコンテンツの購入禁止リストを送信して保持させる。因みに、オフライン機器は、ホームサーバ51に常に接続されているわけではないため、電子配信サービスセンタ1において、コンテンツの購入禁止リストが更新されても、これに応じて内部に保持している購入禁止リストを更新することができない場合がある。

このため、ホームサーバ51は、オフライン機器が接続された場合、相互通信により、互いが保持している購入禁止リストを比較し、当該ホームサーバ51が保持している購入禁止リストが、オフライン機器の保持している購入禁止リストよりも新しい場合には、この購入禁止リストをオフライン機器に送信して更新させる。

また、各オフライン機器同士が接続された場合には、ホームサーバ51と、オフライン機器とが接続された場合と同様に、互いが保持している購入禁止リストを比較し、この結果、互いが保持している購入禁止リストのうちの最新の購入禁止リストを保持しているオフライン機器が相手のオフライン機器に購入禁止リストを送信して更新させ、このようにして、各オフライン機器は、ホームサーバ51に接続されなくても、購入禁止リストを新たなものに更新する。

ところで、ユーザホームネットワーク 5 内の各機器（ホームサーバ 5 1 およびオフライン機器）においては、購入したコンテンツがその購入後に購入禁止となったり、また、購入したコンテンツの提供者（コンテンツプロバイダ 2 およびサービスプロバイダ 3）がコンテンツの購入後に利用中止対象となった場合、当該購入後に購入禁止となったコンテンツや、利用中止となった提供者（コンテンツプロバイダ 2 およびサービスプロバイダ 3）からその利用中止前に購入したコンテンツに対しては、その利用を禁止しないものの、当該コンテンツに対する再配布および再購入を禁止するようになされている。

従って、ユーザホームネットワーク 5 内の各機器（ホームサーバ 5 1 およびオフライン機器）は、既に購入しているコンテンツを再配布および再購入する場合、当該再配布および再購入対象のコンテンツの ID が購入禁止リストに登録されているか否かを検出し、当該購入禁止リストに再配布および再購入対象のコンテンツの ID が登録されていると、このコンテンツの再配布および再購入を行わないようにする。

また、ユーザホームネットワーク 5 内の各機器（ホームサーバ 5 1 およびオフライン機器）は、かかる再配布および再購入の際に、再配布および再購入対象のコンテンツに対応する取扱方針および価格情報に含まれるコンテンツプロバイダの ID およびサービスプロバイダの ID が購入禁止リストに登録されているか否かも検出し、当該購入禁止リストに再配布および再購入対象のコンテンツに対応するコンテンツプロバイダの ID およびサービスプロバイダの ID（すなわち、当該コンテンツの提供者を示す）が登録されていると、このコンテンツの再配布および再購入を行わないようにする。

これに加えて、各機器（ホームサーバ 5 1 およびオフライン機器）は、このように、再配布および再購入の際に、コンテンツの購入禁止リストに基づいて、当該再配布および再購入対象のコンテンツが購入禁止になっていないか否か、当該コンテンツの提供者（コンテンツプロバイダ 2 およびサービスプロバイダ 3）が利用中止対象となっていないか否か検出するものの、このとき保持しているコン

テンツの購入禁止リストが最新のものではないと、再配布および再購入対象のコンテンツが、最新の購入禁止リストでは購入禁止となっていて、それを知らずに相手の機器に送信することが考えられる。

このため、各機器（ホームサーバ51およびオフライン機器）は、コンテンツを再配布および再購入した場合、図109に示すコンテンツの再配布／再購入リストに、当該再配布／再購入リストに、再配布および再購入したコンテンツのID、当該コンテンツの提供者を示すコンテンツプロバイダのIDおよびサービスプロバイダのID、コンテンツの再配布／再購入先の機器に設けられている暗号処理部のIDを登録し、当該再配布／再購入リストを、例えば、大容量記憶部に保存する。因みに、各機器は、コンテンツの再配布および再購入を行う毎に、再配布／再購入リストを更新して保持する。

そして、各機器（ホームサーバ51およびオフライン機器）は、他の機器からコンテンツの購入禁止リストを受け取ったときに（すなわち、ホームサーバ51は電子配信サービスセンタ1から購入禁止リストを受け取ったとき、また、オフライン機器は、ホームサーバ51または他のオフライン機器から購入禁止リストを受け取ったとき）、当該購入禁止リストに登録されている購入禁止対象のコンテンツのID、利用中止対象のコンテンツプロバイダのIDおよびサービスプロバイダのIDに基づいて、再配布／再購入リスト内の情報を検索する。

この結果、各機器（ホームサーバ51およびオフライン機器）は、再配布／再購入リスト内に購入禁止対象のコンテンツのID、利用中止対象のコンテンツプロバイダのIDおよびサービスプロバイダのIDが登録されていると（すなわち、購入禁止対象となったコンテンツ、利用中止対象となった提供者（コンテンツプロバイダ2およびサービスプロバイダ3）から購入したコンテンツが再配布および再購入されていると）、購入禁止対象となったコンテンツまたは、利用中止対象となった提供者（コンテンツプロバイダ2およびサービスプロバイダ3）から購入したコンテンツに対して再配布および再購入を行った相手の機器（ホームサーバ51またはオフライン機器）が更新前の古い購入禁止リストを保持している



可能性が高いと判断し、当該再配布／再購入リスト内の対応する暗号処理部の ID に基づいて、この相手の機器（すなわち、相手の機器が接続されたときに）に購入禁止リストを送信して更新させる。

ここで、ユーザホームネットワーク 5 内の各機器間で行われるコンテンツの再配布および再購入処理を、ホームサーバ 51 の場合について、図 110 に示すフローチャートを用いて説明する。すなわち、ステップ S 890 において、ホームサーバ 51 内の上位コントローラ 62 は、コンテンツの購入禁止リストを大容量記憶部 68 から読み出し、暗号処理部 65 の署名検証ユニット 115 において、この購入禁止リストの署名を検証させ、この結果、購入禁止リストが正しいデータであれば、ステップ S 891 に進む。

ステップ S 891 において、上位コントローラ 62 は、再配布および再購入対象のコンテンツの ID に基づいて、購入禁止リスト内の情報を検索し、当該再配布および再購入対象のコンテンツの ID がこの購入禁止リストに登録されているか否か（すなわち、再配布および再購入対象のコンテンツが購入禁止対象とされていないか否か）を検証し、当該コンテンツの ID が購入禁止リストに登録されていなければ（すなわち、再配布および再購入対象のコンテンツが購入禁止対象にはなっていない）、ステップ S 892 に進む。

ステップ S 892 において、上位コントローラ 62 は、再配布および再購入対象のコンテンツの提供者を示すコンテンツプロバイダの ID（取扱方針に格納されているコンテンツプロバイダの ID）に基づいて、購入禁止リスト内の情報を検索し、当該コンテンツプロバイダの ID が購入禁止リストに登録されているか否か（すなわち、再配布および再購入対象のコンテンツの提供者であるコンテンツプロバイダ 2 が利用中止対象となっていないか否か）を検証し、当該コンテンツプロバイダの ID が購入禁止リストに登録されていなければ（すなわち、再配布および再購入対象のコンテンツの提供者であるコンテンツプロバイダ 2 が利用中止対象となっていない）、ステップ S 893 に進む。

ステップ S 893 において、上位コントローラ 62 は、再配布および再購入対

象のコンテンツの提供者を示すサービスプロバイダのID（価格情報に格納されているサービスプロバイダのID）に基づいて、購入禁止リスト内の情報を検索し、当該サービスプロバイダのIDが購入禁止リストに登録されているか否か（すなわち、再配布および再購入対象のコンテンツの提供者であるサービスプロバイダ3が利用中止対象となっていないか否か）を検証し、当該サービスプロバイダのIDが購入禁止リストに登録されていなければ（すなわち、再配布および再購入対象のコンテンツの提供者であるサービスプロバイダ3が利用中止対象となっていない）、ステップS894に進む。

ステップS894において、上位コントローラ62は、大容量記憶部68からコンテンツの再配布／再購入リストを読み出して暗号処理部65の制御部91に送出し、当該制御部91は、署名検証ユニット115を用いて、この再配布／再購入リストに付加されている署名を検証し、当該再配布／再購入リストが正しいデータであれば、ステップS895に進む。

ステップS895において、上位コントローラ62は、コンテンツの再配布および再購入処理の相手となるオフライン機器から当該オフライン機器の公開鍵証明書が送信されると、これを通信部61によって受信し、当該受信した公開鍵証明書を暗号処理部65の制御部91に送出する。そして、制御部91は、相互認証モジュール95を用いて、この公開鍵証明書により相手のオフライン機器との相互認証を行い、この結果、相手のオフライン機器を認証すると、ステップS896に進み、先ほど検証したコンテンツの再配布／再購入リストに、この公開鍵証明書（ステップS895で相互認証に用いた公開鍵証明書）に含まれるオフライン機器内の暗号処理部のIDを追加登録すると共に、対応する再配布および再購入対象のコンテンツのID、コンテンツプロバイダのIDおよびサービスプロバイダのIDも追加登録してステップS897に進む。

ステップS897において、制御部91は、署名生成ユニット114を用いて、ステップS896において得られた再配布／再購入リストの署名を生成し直し、当該署名を生成し直した再配布／再購入リストを上位コントローラ62を介し

て大容量記憶部 68 に送出し、続くステップ S 898 において、当該大容量記憶部 68 に、この再配布／再購入リストを保存する。

そして、ステップ S 899 において、上位コントローラ 62 は、再配布および再購入対象のコンテンツを再配布および再購入する。

因みに、上位コントローラ 62 は、ステップ S 890 において、購入禁止リストが改竄される等して正しいデータではないと判断すると、ステップ S 900 に進み、当該上位コントローラ 62 から設けられた機器がホームサーバ 51 であるか否かを検出し、この場合、上位コントローラ 62 が設けられた機器は、ホームサーバ 51 であるため、ステップ S 901 に進んで、電子配信サービスセンタ 1 から購入禁止リストを入手し直す。

また、ステップ S 900 では、コンテンツの再配布および再購入処理を実行する機器がオフライン機器であれば、ステップ S 902 に進み、当該コンテンツの再配布および再購入処理を実行する機器が、そのコンテンツの再配布および再購入処理の相手となる機器（ホームサーバ 51 または他のオフライン機器）から購入禁止リストを入手し直す。

そして、ホームサーバ 51 およびオフライン機器は、このように、購入禁止リストを入手し直すと、ステップ S 903 において、当該購入禁止リストの署名を再び検証し、その購入禁止リストが正しいデータであれば、ステップ S 891 に進む。

以上のように、ホームサーバ 51 は、再配布および再購入対象のコンテンツの ID、当該コンテンツの提供者を示すコンテンツプロバイダの ID およびサービスプロバイダの ID が購入禁止リスト内に存在しなければ、当該再配布および再購入対象のコンテンツが購入禁止対象ではなく、かつ、利用中止対象のコンテンツプロバイダ 2 およびサービスプロバイダ 3 から提供されたものでもないと判断し、この再配布および再購入対象のコンテンツを相手のオフライン機器との間で再配布および再購入する。また、ホームサーバ 51 は、この際、コンテンツの再配布／再購入リストを更新して大容量記憶部 68 に保存する。

これに対して、ホームサーバ51内の上位コントローラ62は、ステップS891において、再配布および再購入対象のコンテンツのIDが購入禁止リストに登録されている場合、ステップS892において、当該コンテンツの提供者を示すコンテンツプロバイダのIDが購入禁止リストに登録されている場合、ステップS893において、そのコンテンツの提供者を示すサービスプロバイダのIDが購入禁止リストに登録されている場合には、当該再配布および再購入対象のコンテンツが購入禁止対象であり、または当該コンテンツが利用中止対象のコンテンツプロバイダ2およびサービスプロバイダ3から提供されたものであると判断し、ステップS904においてエラー処理を実行し、かくして、再配布および再購入対象のコンテンツの再配布および再購入を中止する。

因みに、上位コントローラ62は、ステップS894において、コンテンツの再配布／再購入リストの署名の検証の結果、当該再配布／再購入リストが改竄される等して正しくないデータであると判断した場合と、ステップS902において、コンテンツの購入禁止リストの署名の検証の結果、当該購入禁止リストが改竄される等して正しくないデータであると判断した場合にも、エラー処理を実行して当該再配布および再購入対象のコンテンツの再配布および再購入を中止する。

これにより、ホームサーバ51は、購入済みのコンテンツが購入禁止対象となったり、また、当該コンテンツの提供者（コンテンツプロバイダ2およびサービスプロバイダ3）が利用中止対象となっても、このコンテンツを再配布および再購入することを禁止し得る。因みに、ユーザホームネットワーク5内のホームサーバ51を除く他のオフライン機器においても、当該ホームサーバ51と同様に再配布／再購入処理を実行し、かくして、購入禁止対象となった購入済みのコンテンツや、利用中止対象となったコンテンツの提供者（コンテンツプロバイダ2およびサービスプロバイダ3）から購入したコンテンツに対して再配布および再購入を禁止し得る。

なお、ホームサーバ51においては、電子配信サービスセンタ1が所定の送信

手段を介して送信したコンテンツの購入禁止リストを通信部 6 1 によって送信すると、上位コントローラ 6 2 が、このコンテンツの購入禁止リストを暗号処理部 6 5 に送出し、当該暗号処理部 6 5 の署名検証ユニット 1 1 5 により署名の検証を行わせる。次いで、上位コントローラ 6 2 は、大容量記憶部 6 8 からコンテンツの再配布／再購入リストを読み出し、これを暗号処理部 6 5 に送信し、当該暗号処理部 6 5 の署名検証ユニット 1 1 5 に署名の検証を行わせる。

そして、上位コントローラ 6 2 は、コンテンツの購入禁止リストに登録されている購入禁止対象のコンテンツの ID が再配布／再購入リストに登録されている場合には、当該購入禁止リストを、この購入禁止対象のコンテンツを再配布および再購入した相手のオフライン機器等に送信し、かくして、相手のオフライン機器に購入禁止リストを更新させる。同様に、上位コントローラ 6 2 は、購入禁止リストに登録されている利用中止対象となっているコンテンツプロバイダの ID またはサービスプロバイダの ID が、コンテンツの再配布／再購入リストに登録されている場合には、当該購入禁止リストを、利用中止対象となったコンテンツプロバイダ 2 またはサービスプロバイダ 3 から購入したコンテンツを再配布および再購入した相手のオフライン機器等に送信し、かくして、相手のオフライン機器に購入禁止リストを更新させる。

このように、電子配信サービスセンタ 1 にオンライン接続されたホームサーバ 5 1 と、オフライン機器との間では、購入禁止リストを入手する毎に当該購入禁止リストに基づいて再配布／再購入リスト内の検索処理を実行することにより、既に再配布および再購入したコンテンツが購入禁止対象となり、または当該コンテンツの提供者（コンテンツプロバイダ 2 およびサービスプロバイダ 3）が利用中止対象となっても、当該コンテンツが再び再配布および再購入することを未然に防止し得る。

因みに、各オフライン機器同士の間でも、ホームサーバ 5 1 およびオフライン機器との間で行われる再配布／再購入リスト内の検索処理と同様の処理を実行することにより、既に再配布および再購入したコンテンツが購入禁止対象となり、

または当該コンテンツの提供者（コンテンツプロバイダ 2 およびサービスプロバイダ 3）が利用中止対象となっても、当該コンテンツが再び再配布および再購入することを未然に防止し得る。

以上の構成において、電子音楽配信システム 10 では、電子配信サービスセンタ 1 により、コンテンツの購入禁止リストを作成し、当該作成した購入禁止リストを当該電子配信サービスセンタ 1 とオンライン接続されたユーザホームネットワーク 5 内のホームサーバ 51 に送信する。また、ユーザホームネットワーク 5 内では、ホームサーバ 51 が電子配信サービスセンタ 1 にオンライン接続されていないオフライン機器にコンテンツの購入禁止リストを送信すると共に、これら各オフライン機器間でも、通信の際に互いに保持している購入禁止リストを比較し、いずれか一方が他方よりも新しく更新した購入禁止リストであれば、互いにこの新しい購入禁止リストを保持するようにする。

そして、ユーザホームネットワーク 5 内では、各機器（ホームサーバ 51 およびオフライン機器）がコンテンツプロバイダ 2 からサービスプロバイダ 3 を介してコンテンツが配信された場合、またはユーザホームネットワーク 5 内の他の機器からコンテンツが送信された場合、購入禁止リストを用いて、このコンテンツが購入禁止対象であるか否か、当該コンテンツの提供者であるコンテンツプロバイダ 2 や、サービスプロバイダ 3 が利用禁止対象となっているか否かを判断し、当該コンテンツが購入禁止対象であり、またはコンテンツの提供者であるコンテンツプロバイダ 2 およびサービスプロバイダ 3 が利用禁止対象であるときには、このコンテンツを購入を中止する。

従って、かかる電子音楽配信システム 10 では、ユーザホームネットワーク 5 内の各機器（ホームサーバ 51 およびオフライン機器）が購入禁止対象のコンテンツや、利用禁止対象のコンテンツプロバイダ 2 およびまたはサービスプロバイダ 3 から提供されたコンテンツが購入されることを防止することができる。

また、電子音楽配信システム 10 では、ユーザホームネットワーク 5 内の機器間で再配布および再購入したコンテンツが購入禁止対象となり、または当該コン

テンツの提供者であるコンテンツプロバイダ 2、サービスプロバイダ 3 が利用中止対象となった場合、当該機器がコンテンツの再配布／再購入リスト内の暗号処理部の ID に基づいて、コンテンツの再配布および再購入処理を実行した相手の機器に購入禁止リストを送信するため、相手の機器から不正なコンテンツが他の機器に拡散することを未然に防止することができる。

以上の構成によれば、電子配信サービスセンタ 1 においてコンテンツの購入禁止リストを作成し、当該購入禁止リストをユーザホームネットワーク 5 内の各機器（ホームサーバ 5 1 およびオフライン機器）が保持し、当該ユーザホームネットワーク 5 内の各機器がこの購入禁止リストに基づいて、購入禁止対象のコンテンツおよび、利用禁止対象のコンテンツプロバイダ 2 やサービスプロバイダ 3 から送信されたコンテンツの購入を中止するようにしたことにより、ユーザホームネットワーク 5 内の各機器において、購入禁止対象のコンテンツや、利用禁止対象のコンテンツプロバイダ 2 およびまたはサービスプロバイダ 3 から提供されたコンテンツが購入されることを防止することができ、かくして提供禁止対象のコンテンツが利用されることをほぼ確実に防止し得る電子音楽配信システムを実現することができる。

因みに、購入禁止リストには、購入禁止対象のコンテンツの ID、利用禁止対象のコンテンツプロバイダ 2 およびサービスプロバイダ 3 の ID をそれぞれ登録するようにしたが、少なくとも購入禁止対象のコンテンツの ID が登録されていれば良い。

また、ユーザホームネットワーク 5 内の各機器では、コンテンツの購入禁止リストを大容量記憶部に保持するようにしたが、当該購入禁止リストを外部メモリ等のように、この他種々の記録媒体に保持しても良い。

さらに、ユーザホームネットワーク 5 内の各機器では、暗号処理部が購入禁止リストに基づいて、購入するコンテンツが購入禁止対象であるか否かを判断するようにしたが、この判断処理を上位コントローラによって実行しても良い。

さらに、かかる電子音楽配信システム 10 では、当該システム内に不当なコン

テンツが流入した際に、当該コンテンツのIDを突き止めることができれば、この不当なコンテンツがユーザホームネットワーク5内の機器で購入されることも防止することができる。

さらに、ユーザホームネットワーク5内の機器において、購入禁止リストを検証することにより購入禁止対象のコンテンツを保持していることが判明した場合には、当該コンテンツに対応する使用許諾条件情報内の所定の領域に、当該コンテンツの再配布および再購入を禁止することを示す情報を埋め込むようにしても良い。同様に、利用禁止対象のコンテンツプロバイダ2およびサービスプロバイダ3から購入したコンテンツに対しても、当該コンテンツに対応する使用許諾条件情報内の所定の領域に当該コンテンツの再配布および再購入を禁止することを示す情報を埋め込むようにしても良い。これにより、再配布および再購入の際にコンテンツの購入禁止リスト内を検索しなくても、対応する使用許諾条件情報を見ることで、再配布および再購入禁止対象のコンテンツを容易に識別することができる。

### (13) 電子音楽配信システムの他の構成

図111は、他の構成の電子音楽配信システム400を説明する図である。かかる電子音楽配信システム400においては、パーソナルコンピュータ構成の電子配信サービスセンタ401に、コンテンツサーバ用及び信号処理用の2台のパーソナルコンピュータ402および403からなるコンテンツプロバイダ404と、同様にコンテンツサーバ用及び信号処理用の2台のパーソナルコンピュータ405および406からなるサービスプロバイダ407との信号処理用のパーソナルコンピュータ（以下、これを信号処理用パーソナルコンピュータと呼ぶ）403および406が接続されている。

また、サービスプロバイダ407の信号処理用パーソナルコンピュータ406には、コンテンツプロバイダ404の信号処理用パーソナルコンピュータ403が接続されると共に、ユーザホームネットワーク408に設けられたパーソナルコンピュータ構成のホームサーバ409がネットワーク4を介して接続されてい



る。

そして、ユーザホームネットワーク 408 においては、ホームサーバ 409 に据置型の記録再生装置などの据置機器 410 と、携帯型の記録再生装置や携帯型の通信端末（携帯型情報機器や携帯電話機など）などの携帯機器 411 とが接続されて構成されている。

図 112 に示すように、電子配信サービスセンタ 401 においては、CPU (Central Processing Unit) などの制御部 415 にバス 416 を介して RAM (Random Access Memory) 417、ROM (Read Only Memory) 418、表示部 419、入力部 420、ハードディスクドライブ (HDD: Hard Disk Drive) 421 およびネットワークインターフェイス 422 が接続されて構成されている。

この場合、制御部 415 は、ROM 418 に予め格納された各種プログラムを読み出して RAM 417 上で展開することによりこれら各種プログラムに従って図 2 について上述した電子配信サービスセンタ 1 のサービスプロバイダ管理部 11、コンテンツプロバイダ管理部 12、著作権管理部 13、鍵サーバ 14、経歴データ管理部 15、利益配分部 16、相互認証部 17、ユーザ管理部 18、課金請求部 19、出納部 20 および監査部 21 と同様の処理を実行し得るようになされている。

また、制御部 415 は、システム全てに使用する鍵（配送鍵  $K_d$  および個別鍵  $K_i$  など）や、課金情報、価格情報、取扱方針、さらにはユーザ登録データベース等の各種情報をハードディスクドライブ 421 のハードディスクに記録することによりこれら各種情報を保持・管理している。

さらに、制御部 415 は、ネットワークインターフェイス 422 を介してコンテンツプロバイダ 404、サービスプロバイダ 407、ユーザホームネットワーク 408 および JASRAC などと通信し得るようになされており、これにより、コンテンツプロバイダ 404、サービスプロバイダ 407、ユーザホームネットワーク 408 および JASRAC などとの間で配送鍵  $K_d$ 、配送鍵  $K_d$  で暗号化

した個別鍵 $K_i$ 、課金情報、価格情報、取扱方針、登録情報およびコンテンツの利用実績などの各種情報を授受し得るようになされている。

このようにしてパーソナルコンピュータ構成の電子配信サービスセンタ401は、各種プログラムに従って、図2について上述した電子配信サービスセンタ1と同様の機能を実現し得るようになされている。

因みに、電子配信サービスセンタ401においては、入力部420および表示部419を特には使用しないことによりこれら入力部420および表示部419を設けないようにしても良いが、ハードディスクドライブ421に記録している各種情報などを確認するためなどに入力部420および表示部419を使用しても良い。

また、電子配信サービスセンタ401においては、ROM418に代えて各種プログラムをハードディスクドライブ421のハードディスクに予め記録しても良い。

図113は、コンテンツプロバイダ404の構成を示すブロック図であり、コンテンツサーバ用のパーソナルコンピュータ（以下、これをサーバ用パーソナルコンピュータと呼ぶ）402は、CPUなどの制御部425にバス426を介してRAM427、ROM428、表示部429、入力部430、ユーザに供給するコンテンツをハードディスクに記憶しているハードディスクドライブ431およびIEEE（Institute of Electrical and Electronics Engineers）1394インターフェイス432が接続されて構成されている。

また、コンテンツプロバイダ404において、信号処理用パーソナルコンピュータ403は、CPUなどの制御部435にバス436を介してRAM437、ROM438、表示部439、入力部440、ハードディスクドライブ441、電子配信サービスセンタ401およびサービスプロバイダ407との接続用のネットワークインターフェイス442、サーバ用パーソナルコンピュータ402のIEEE1394インターフェイス432とIEEE1394ケーブル443を

介して接続されるIEEE1394インターフェイス444が接続されて構成されている。

この場合、サーバ用パーソナルコンピュータ402の制御部425は、ROM428に予め格納された所定のプログラムを読み出してRAM427上で展開することにより当該プログラムに従って動作しており、信号処理用パーソナルコンピュータ403の制御部435からIEEE1394ケーブル443を介してコンテンツの読出命令が送信されると、その読出命令をIEEE1394インターフェイス432を介して取り込み、当該取り込んだコンテンツの読出命令に基づいてハードディスクドライブ431のハードディスクからコンテンツを読み出すと共に、その読み出したコンテンツをIEEE1394インターフェイス432からIEEE1394ケーブル443を介して信号処理用パーソナルコンピュータ403に送信する。

因みに、サーバ用パーソナルコンピュータ402においては、入力部430および表示部429を特には使用しないことによりこれら入力部430および表示部429を設けないようにしても良いが、ハードディスクドライブ431に記録しているコンテンツを確認したり、またはハードディスクドライブ431に新たにコンテンツを記憶したりコンテンツを削除する場合などに入力部430および表示部429を使用しても良い。

また、サーバ用パーソナルコンピュータ402においては、ROM428に代えてプログラムをハードディスクドライブ431のハードディスクに予め記録するようにしても良い。

一方、コンテンツプロバイダ404において、信号処理用パーソナルコンピュータ403の制御部435は、個別鍵 $K_i$ 、配送鍵 $K_d$ で暗号化された個別鍵 $K_i$ 、コンテンツプロバイダ404の公開鍵証明書をハードディスクドライブ439のハードディスクに記録することによりこれら個別鍵 $K_i$ 、配送鍵 $K_d$ で暗号化された個別鍵 $K_i$ 、コンテンツプロバイダ404の公開鍵証明書を保持・管理している。

そして、制御部 4 3 5 は、ROM 4 3 8 に予め格納された所定の各種プログラムを読み出して RAM 4 3 7 上で展開することによりこれら各種プログラムに従って、図 9 について上述したコンテンツプロバイダ 2 の電子透かし付加部 3 2、圧縮部 3 3、コンテンツ暗号部 3 4、コンテンツ鍵生成部 3 5、コンテンツ鍵暗号部 3 6、取扱方針生成部 3 7、署名生成部 3 8 および相互認証部 3 9 と同様の処理を実行し得るようになされている。

これにより、信号処理用パーソナルコンピュータ 4 0 3 は、配送鍵  $K_d$ 、配送鍵  $K_d$  で暗号化した個別鍵  $K_i$ 、取扱方針、コンテンツプロバイダセキュアコンテナを電子配信サービスセンタ 4 0 1 およびサービスプロバイダ 4 0 7 との間でネットワークインターフェイス 4 4 2 を介して授受し得るようになされている。

このようにしてパーソナルコンピュータ構成のコンテンツプロバイダ 4 0 4 は、各種プログラムに従って、図 9 について上述したコンテンツプロバイダ 2 と同様の機能を実現し得るようになされている。

因みに、信号処理用パーソナルコンピュータ 4 0 3 においては、入力部 4 4 0 および表示部 4 3 9 を特には使用しないことによりこれら入力部 4 4 0 および表示部 4 3 9 を設けないようにしても良いが、ハードディスクドライブ 4 4 1 に記録している個別鍵  $K_i$ 、配送鍵  $K_d$  で暗号化された個別鍵  $K_i$ 、コンテンツプロバイダ 4 0 4 の公開鍵証明書などを確認するためなどに入力部 4 4 0 および表示部 4 3 9 を使用しても良い。

また、信号処理用パーソナルコンピュータ 4 0 3 においては、ROM 4 3 8 に代えて各種プログラムをハードディスクドライブ 4 4 1 のハードディスクに予め記録するようにしても良い。さらに、信号処理用パーソナルコンピュータ 4 0 3 においては、RAM 4 3 7 に耐タンパ性をもたせて個別鍵  $K_i$  を保持するようにしても良い。

さらに、コンテンツプロバイダ 4 0 4 においては、信号処理用パーソナルコンピュータ 4 0 3 と、サーバ用パーソナルコンピュータ 4 0 2 とを IEEE 1394 ケーブル 4 4 3 を介して接続するようにしたが、当該信号処理用パーソナルコ

ンピュータ４０３と、サーバ用パーソナルコンピュータ４０２とをUSB（Universal Serial Bus）ケーブルやRS-232Cケーブルなどの所定の信号ケーブルなどを介して有線接続したり、所定の無線通信手段を介して無線接続するようにしても良い。

図１１４は、サービスプロバイダ４０７の構成を示すブロック図であり、サーバ用パーソナルコンピュータ４０５は、CPUなどの制御部４４５にバス４４６を介してRAM４４７、ROM４４８、表示部４４９、入力部４５０、コンテンツプロバイダセキュアコンテナおよびコンテンツプロバイダ４０４の公開鍵証明書をハードディスクに記憶しているハードディスクドライブ４５１、IEEE 1394 インターフェイス４５２が接続されて構成されている。

また、サービスプロバイダ４０７において、信号処理用パーソナルコンピュータ４０６は、CPUなどの制御部４５４にバス４５５を介してRAM４５６、ROM４５７、表示部４５８、入力部４４９、ハードディスクドライブ４６０、電子配信サービスセンタ４０１およびコンテンツプロバイダ４０４との接続用のネットワークインターフェイス４６１、サーバ用パーソナルコンピュータ４０５のIEEE 1394 インターフェイス４５２とIEEE 1394 ケーブル４６２を介して接続されるIEEE 1394 インターフェイス４６３、ユーザホームネットワーク４０８とネットワーク４を介して接続するためのモデム４６４が接続されて構成されている。

この場合、サーバ用パーソナルコンピュータ４０５の制御部４４５は、ROM ４４８に予め格納された所定のプログラムを読み出してRAM４４７上で展開することにより当該プログラムに従って動作しており、信号処理用パーソナルコンピュータ４０６の制御部４５４からIEEE 1394 ケーブル４６２を介してコンテンツプロバイダセキュアコンテナおよびコンテンツプロバイダ４０４の公開鍵証明書と共にこれらの書込命令が与えられると、IEEE 1394 インターフェイス４５２を介して取り込み、当該取り込んだ書込命令に基づいてハードディスクドライブ４５１のハードディスクにコンテンツプロバイダセキュアコンテナ

およびコンテンツプロバイダ 404 の公開鍵証明書を書き込むと共に、信号処理用パーソナルコンピュータ 406 の制御部 454 から IEEE 1394 ケーブル 462 を介してコンテンツプロバイダセキュアコンテナおよびコンテンツプロバイダ 404 の公開鍵証明書の読出命令が与えられると、その読出命令を IEEE 1394 インターフェイス 452 を介して取り込み、当該取り込んだ読出命令に基づいてハードディスクドライブ 451 のハードディスクからコンテンツプロバイダセキュアコンテナおよびコンテンツプロバイダ 404 の公開鍵証明書を読み出すと共に、その読み出したコンテンツプロバイダセキュアコンテナおよびコンテンツプロバイダ 404 の公開鍵証明書を IEEE 1394 インターフェイス 452 から IEEE 1394 ケーブル 462 を介して信号処理用パーソナルコンピュータ 406 に送信する。

因みに、サーバ用パーソナルコンピュータ 405 においては、入力部 450 および表示部 449 を特には使用しないことによりこれら入力部 450 および表示部 449 を設けないようにしても良いが、ハードディスクドライブ 451 に記録しているコンテンツプロバイダセキュアコンテナおよびコンテンツプロバイダ 404 の公開鍵証明書などを確認するなどのために入力部 450 および表示部 449 を使用しても良い。

また、サーバ用パーソナルコンピュータ 405 においては、ROM 448 に代えてプログラムをハードディスクドライブ 451 のハードディスクに予め記録するようにしても良い。

一方、サービスプロバイダ 407 において、信号処理用パーソナルコンピュータ 406 の制御部 454 は、サービスプロバイダ 407 の公開鍵証明書をハードディスクドライブ 460 のハードディスクに記録し、RAM 456 に耐タンパ性をもたせてサービスプロバイダ 407 の秘密鍵を保持・管理している。

そして、制御部 454 は、ROM 457 に予め格納された所定の各種プログラムを読み出して RAM 456 上で展開することによりこれら各種プログラムに従って、図 14 について上述したサービスプロバイダ 3 の証明書検証部 42、署名

検証部 4 3、値付け部 4 4、署名生成部 4 5 および相互認証部 4 6 と同様の処理を実行し得るようになされている。

これにより、信号処理用パーソナルコンピュータ 4 0 6 は、価格情報、コンテンツプロバイダセキュアコンテナなどを電子配信サービスセンタ 4 0 1 およびコンテンツプロバイダ 4 0 7 との間でネットワークインターフェイス 4 4 2 を介して授受し得ると共に、サービスプロバイダセキュアコンテナをモデム 4 6 4 を介してユーザホームネットワーク 4 0 8 に送信し得るようになされている。

このようにしてパーソナルコンピュータ構成のサービスプロバイダ 4 0 7 は、各種プログラムに従って、図 1 4 について上述したサービスプロバイダ 3 と同様の機能を実現し得るようになされている。

因みに、信号処理用パーソナルコンピュータ 4 0 6 においては、入力部 4 5 9 および表示部 4 5 8 を特には使用しないことによりこれら入力部 4 5 9 および表示部 4 5 8 を設けないようにしても良いが、ハードディスクドライブ 4 6 0 に記録しているサービスプロバイダ 4 0 7 の公開鍵証明書などを確認するためなどに入力部 4 5 9 および表示部 4 5 8 を使用しても良い。

また、信号処理用パーソナルコンピュータ 4 0 6 においては、ROM 4 5 7 に代えて各種プログラムをハードディスクドライブ 4 6 0 のハードディスクに予め記録するようにしても良い。

さらに、サービスプロバイダ 4 0 7 においては、信号処理用パーソナルコンピュータ 4 0 6 と、サーバ用パーソナルコンピュータ 4 0 5 とを IEEE 1394 ケーブル 4 6 2 を介して接続するようにしたが、当該信号処理用パーソナルコンピュータ 4 0 6 と、サーバ用パーソナルコンピュータ 4 0 5 とを USB ケーブルや RS-232C ケーブルなどの所定の信号ケーブルなどを介して有線接続したり、所定の無線通信手段を介して無線接続するようにしても良い。

図 1 1 5 は、ユーザホームネットワーク 4 0 8 の構成を示すブロック図であり、パーソナルコンピュータ構成のホームサーバ 4 0 9 は、CPU などの制御部 4 6 5 にバス 4 6 6 を介して RAM 4 6 7、ROM 4 6 8、表示部 4 6 9、入力部

４７０、ハードディスクドライブ４７１、ＩＥＥＥ１３９４インターフェイス４７２、サービスプロバイダ４０７とネットワーク４を介して接続するためのモデム４７３、電子配信サービスセンタ４０１との接続用のネットワークインターフェイス４７４が接続されて構成されている。

また、ユーザホームネットワーク４０８において、据置機器４１０は、ＣＰＵなどの制御部４７５にバス４７６を介してＲＡＭ４７７、ＲＯＭ４７８、表示部４７９、入力部４８０、記録再生部４８１、記録メディア４８２用のメディアインターフェイス４８３、ホームサーバのＩＥＥＥ１３９４インターフェイス４７２とＩＥＥＥ１３９４ケーブル４８４を介して接続されるＩＥＥＥ１３９４インターフェイス４８５が接続されて構成されている。

さらに、ユーザホームネットワーク４０８において、携帯機器４１１は、ＣＰＵなどの制御部４９０にバス４９１を介してＲＡＭ４９２、ＲＯＭ４９３、表示部４９４、入力部４９５、ホームサーバのＩＥＥＥ１３９４インターフェイス４７２とＩＥＥＥ１３９４ケーブル４９６を介して接続されるＩＥＥＥ１３９４インターフェイス４９７が接続されて構成されている。

この場合、ホームサーバ４０９の制御部４６５は、ＲＯＭ４６８に予め格納された各種プログラムを読み出してＲＡＭ４６７上で展開することによりこれら各種プログラムに従って図１５について上述したホームサーバ５１の上位コントローラ６２、暗号処理部６５および伸張部６６と同様の処理を実行し得るようになっている。

また、ホームサーバ４０９の表示部４６９は、図１５について上述したホームサーバ５１の表示手段６４と同様の機能を有し、当該ホームサーバ４０９の入力部４７０は、図１５について上述したホームサーバ５１の入力手段６３と同様の機能を有している。さらに、ホームサーバ４０９のハードディスクドライブ４７１は、図１５について上述したホームサーバ５１の大容量記憶部６８と同様の機能を有すると共に、モデム４７３およびネットワークインターフェイス４７４並びにＩＥＥＥ１３９４インターフェイス４７２は、図１５について上述したホー



ムサーバ51の通信部61と同様の機能を有し、当該ホームサーバ409のRAM467は、図15について上述したホームサーバ51の外部メモリ67と同様の機能を有している。

従って、パーソナルコンピュータ構成のホームサーバ409は、各種プログラムに従って、図15について上述したホームサーバ51と同様の機能を実現し得るようになされている。

因みに、ホームサーバ409においては、ROM468に代えて各種プログラムをハードディスクドライブ471のハードディスクに予め記録したり、当該ハードディスクドライブ471を図15について上述した外部メモリ67と同様に機能させても良い。また、ホームサーバ409においては、サービスプロバイダ407および電子配信サービスセンタ401との通信形態によってはモデム473およびネットワークインターフェイス474を1つのモデムなどのインターフェイスとしても良い。さらに、ホームサーバ409においては、据置機器410および携帯機器411をUSBケーブルやRS-232Cケーブルなどの所定の信号ケーブルなどを介して有線接続したり、所定の無線通信手段を介して無線接続するようにしても良い。

一方、ユーザホームネットワーク408において、据置機器410の制御部475は、ROM478に予め格納された各種プログラムを読み出してRAM477上で展開することによりこれら各種プログラムに従って図15について上述した据置機器52の上位コントローラ72、暗号処理部73および伸張部74と同様の処理を実行し得るようになされている。

また、据置機器410の表示部479は、図15について上述した据置機器52の表示手段78と同様の機能を有すると共に、入力部480は、図15について上述した据置機器52の入力手段77と同様の機能を有し、IEEE1394インターフェイス485は、図15について上述した据置機器52の通信部71と同様の機能を有している。さらに、据置機器410の記録再生部481は、図15について上述した据置機器52の記録再生部76と同様の機能を有すると共

に、記録メディア 482 は、図 15 について上述した据置機器 52 の記録メディア 80 と同様の機能を有し、当該据置機器 410 の RAM 477 は、図 15 について上述した据置機器 52 の外部メモリ 79 および小容量記憶部 75 と同様の機能を有している。

従って、ユーザホームネットワーク 408 の据置機器 410 は、各種プログラムに従って、図 15 について上述したユーザホームネットワーク 5 の据置機器 52 と同様の機能を実現し得るようになされている。

因みに、据置機器 410 においては、ハードディスクドライブを新たに設け、ROM 478 に代えて各種プログラムをそのハードディスクドライブのハードディスクに予め記録したり、当該ハードディスクドライブを図 15 について上述した据置機器 52 の外部メモリ 79 および小容量記憶部 75 と同様に機能させても良い。また、据置機器 410 においては、記録メディア 482 が半導体メモリ構成である場合には、所定のプログラムに従って制御部 475 に記録再生部 481 の機能を実現させても良い。

ユーザホームネットワーク 408 において、携帯機器 411 の制御部 490 は、ROM 493 に予め格納された各種プログラムを読み出して RAM 492 上で展開することによりこれら各種プログラムに従って図 15 について上述した携帯機器 53 の上位コントローラ 82、暗号処理部 83 および伸張部 84 と同様の処理を実行し得るようになされている。

また、携帯機器 411 の RAM 492 は、図 15 について上述した携帯機器 53 の外部メモリ 85 と同様の機能を有し、IEEE 1394 インターフェイス 497 は、図 15 について上述した携帯機器 53 の通信部 81 と同様の機能を有している。さらに、この携帯機器 411 では、表示部 494 および入力部 495 をコンテンツの再生時に利用し得るようになされている。

従って、ユーザホームネットワーク 408 の携帯機器 411 は、各種プログラムに従って、図 15 について上述したユーザホームネットワーク 5 の携帯機器 53 と同様の機能を実現し得るようになされている。

因みに、携帯機器 411 においては、コンテンツの記録再生用に着脱自在な記録メディアを設けるようにしても良い。

以上の構成において、かかる電子音楽配信システム 400 においては、電子配信サービスセンタ 401、コンテンツプロバイダ 404、サービスプロバイダ 407 およびユーザホームネットワーク 408 のホームサーバ 409 をそれぞれパーソナルコンピュータ構成とした。

従って、電子音楽配信システム 400 では、コンテンツの配信用として、電子配信サービスセンタ 401、コンテンツプロバイダ 404、サービスプロバイダ 407 およびホームサーバ 409 をハード構成で新たに製作する必要がなく、既存のパーソナルコンピュータに各種プログラムをインストールするだけで、これらパーソナルコンピュータを用いてシステムを容易に構築することができる。

以上の構成によれば、パーソナルコンピュータ構成の電子配信サービスセンタ 401、コンテンツプロバイダ 404、サービスプロバイダ 407 およびホームサーバ 409 を用いて電子音楽配信システム 400 を構築するようにしたことにより、既存のパーソナルコンピュータを容易に電子配信サービスセンタ 401、コンテンツプロバイダ 404、サービスプロバイダ 407 およびホームサーバ 409 とすることができ、かくして、システム構築を容易、かつ簡易にし得る。

なお、かかる電子音楽配信システム 400 では、電子配信サービスセンタ 401、コンテンツプロバイダ 404、サービスプロバイダ 407、ホームサーバ 409、据置機器 410 および携帯機器 411 を ROM 418、428、438、448、457、468、478、493 に予め格納された各種プログラムに従って動作させるようにした場合について述べたが、各種プログラムが記録されたプログラム格納媒体を電子配信サービスセンタ 401、コンテンツプロバイダ 404、サービスプロバイダ 407、ホームサーバ 409、据置機器 410 および携帯機器 411 にインストールすることにより、当該電子配信サービスセンタ 401、コンテンツプロバイダ 404、サービスプロバイダ 407、ホームサーバ 409、据置機器 410 および携帯機器 411 をプログラム格納媒体に格納して

いる各種プログラムや、当該プログラム格納媒体からハードディスクなどに移行させた各種プログラムに従ってそれぞれ動作させるようにしても良い。

因みに、電子配信サービスセンタ 401、コンテンツプロバイダ 404、サービスプロバイダ 407、ホームサーバ 409、据置機器 410 および携帯機器 411 を動作させるために用いるプログラム格納媒体としては、CD-ROM (Compact Disc-Read Only Memory) などのパッケージメディアのみならず、プログラムが一時的もしくは永続的に格納される半導体メモリや磁気ディスクなどで実現しても良い。また、これらプログラム格納媒体にプログラムを格納する手段としては、ローカルエリアネットワークやインターネット、デジタル衛星放送などの有線および無線通信媒体を利用しても良く、ルータやモデムなどの各種通信インターフェイスを介在させて格納するようにしても良い。

#### 産業上の利用可能性

本発明は、音楽、映像、ゲームプログラムなどのコンテンツを提供するプロバイダなどの情報送信装置や、当該提供されたコンテンツを受信するパーソナルコンピュータや携帯電話機などの情報受信装置、さらには、これら情報送信装置及び情報受信装置から構築されるネットワークシステムに利用することができる。

## 請 求 の 範 囲

1. 情報送信装置から所定のコンテンツデータを情報受信装置に送信する情報送信システムにおいて、

上記情報送信装置は、

上記情報受信装置固有の配送鍵で暗号化した、上記情報送信装置を識別するための識別情報を保持する識別情報保持手段と、

上記配送鍵で暗号化した上記識別情報と比較するために上記コンテンツデータに上記識別情報を付加する識別情報付加手段と、

上記識別情報を付加した上記コンテンツデータと共に、上記配送鍵で暗号化された上記識別情報を送信する送信手段とを具え、

上記情報受信装置は、

上記配送鍵を保持する配送鍵保持手段と、

上記識別情報が付加された上記コンテンツデータ及び上記配送鍵で暗号化された上記識別情報を受信する受信手段と、

上記配送鍵で暗号化された上記識別情報を当該配送鍵で復号化する復号化手段と、

上記コンテンツデータに付加された上記識別情報と、上記復号された上記識別情報とを比較する比較手段とを具える。

2. 請求の範囲第1項に記載の情報送信システムにおいて、

上記情報送信装置は、

上記コンテンツデータに対する使用条件を規定し、上記識別情報を格納したコンテンツ取扱方針を生成する取扱方針生成手段を具え、

上記識別情報付加手段は、上記コンテンツデータに上記コンテンツ取扱方針を付加する。



3. 請求の範囲第1項に記載の情報送信システムにおいて、

上記情報送信装置の上記識別情報付加手段は、上記コンテンツデータに上記識別情報を直接付加する。

4. 請求の範囲第1項に記載の情報送信システムにおいて、

上記情報送信装置は、

上記コンテンツデータを所定のコンテンツ鍵で暗号化するコンテンツデータ暗号化手段と、

上記コンテンツ鍵を所定の個別鍵で暗号化するコンテンツ鍵暗号化手段と、

上記個別鍵で暗号化した上記コンテンツ鍵及び上記配送鍵で暗号化した上記識別情報に、不正データ及び改竄をチェックするための署名データを付加する署名付加手段とを具え、

上記情報受信装置は、

上記署名データを検証する署名検証手段を具える。

5. 請求の範囲第4項に記載の情報送信システムにおいて、

上記情報送信装置の上記署名付加手段は、上記コンテンツ鍵で暗号化された上記コンテンツデータに上記署名データを付加すると共に、当該署名データを付加した、上記コンテンツ鍵で暗号化された上記コンテンツデータを複数格納してなるアルバムコンテンツデータが生成された際には、当該アルバムコンテンツデータにも上記署名データを付加し、

上記情報受信装置の上記署名検証手段は、上記アルバムコンテンツデータに付加された上記署名データを検証し、当該検証の結果、上記アルバムコンテンツデータが正しいデータであると判断したときには、当該アルバムコンテンツデータに格納された上記コンテンツ鍵で暗号化された各上記コンテンツデータに付加された上記署名データの検証を省略する。

6. 請求の範囲第5項に記載の情報送信システムにおいて、

上記情報送信装置の上記署名付加手段は、上記個別鍵で暗号化したコンテンツ鍵及び上記配送鍵で暗号化した上記識別情報にそれぞれ上記署名データを付加し、上記アルバムコンテンツデータに対応させて、上記署名データを付加した上記個別鍵で暗号化したコンテンツ鍵及び上記配送鍵で暗号化した上記識別情報を複数格納してアルバム用鍵データが生成された際には、当該アルバム用鍵データにも上記署名データを付加し、

上記情報受信装置の上記署名検証手段は、上記アルバム鍵データに付加された上記署名データを検証し、当該検証の結果、上記アルバム鍵データが正しいデータであると判断したときには、当該アルバム鍵データに格納された、上記個別鍵で暗号化したコンテンツ鍵及び上記配送鍵で暗号化した上記識別情報にそれぞれ付加された上記署名データの検証を省略する。

7. 請求の範囲第6項に記載の情報送信システムにおいて、

上記情報送信装置は、

上記コンテンツデータの使用条件を規定し、上記識別情報を格納したコンテンツ取扱方針を生成する取扱方針生成手段を具え、

上記情報送信装置の上記署名付加手段は、上記コンテンツ取扱方針に上記署名データを付加し、上記アルバムコンテンツデータに対応させて、上記署名データを付加した上記コンテンツ取扱方針を複数格納してアルバム取扱方針が生成された際には、当該アルバム取扱方針にも上記署名データを付加し、

上記情報受信装置の上記署名検証手段は、上記アルバム取扱方針に付加された上記署名データを検証し、当該検証の結果、上記アルバム取扱方針が正しいデータであると判断したときには、当該アルバム取扱保身に格納された上記コンテンツ取扱方針に付加された上記署名データの検証を省略する。

8. 請求の範囲第7項に記載の情報送信システムにおいて、



上記情報送信装置は、

上記コンテンツデータに対する価格を示すコンテンツ価格情報を作成する価格情報作成手段を具え、

上記情報送信装置の上記署名付加手段は、上記コンテンツ価格情報に上記署名データを付加し、上記アルバムコンテンツデータに対応させて、上記署名データを付加した上記コンテンツ価格情報を複数格納したアルバム価格情報データが生成された際には、当該アルバム価格情報にも上記署名データを付加し、

上記情報受信装置の上記署名検証手段は、上記アルバム価格情報に付加された上記署名データを検証し、当該検証の結果、上記アルバム価格情報が正しいデータであると判断したときには、当該アルバム価格情報に格納された上記コンテンツ価格情報に付加された上記署名データの検証を省略する。

9. 請求の範囲第8項に記載の情報送信システムにおいて、

上記情報送信装置の上記取扱方針生成手段は、上記コンテンツ鍵で暗号化された上記コンテンツデータに付加した上記署名データの検証の有無を表す署名検証情報を格納した上記コンテンツ取扱方針を生成し、

上記情報受信装置の上記署名検証手段は、上記コンテンツ取扱方針に格納された上記署名検証情報に基づいて、上記コンテンツ鍵で暗号化された上記コンテンツデータに付加した上記署名データを検証するように指定されたときのみ、当該コンテンツ鍵で暗号化された上記コンテンツデータに付加した上記署名データを検証する。

10. 請求の範囲第9項に記載の情報送信システムにおいて、

上記情報送信装置の上記取扱方針生成手段は、上記アルバムコンテンツデータに付加した上記署名データの検証の有無を表す上記署名検証情報を格納した上記コンテンツ取扱方針を生成し、

上記情報受信装置の上記署名検証手段は、上記コンテンツ取扱方針に格納され

た上記署名検証情報に基づいて、上記アルバムコンテンツデータに付加した上記署名データを検証するように指定されたときのみ、当該アルバムコンテンツデータに付加した上記署名データを検証する。

1 1. 請求の範囲第 8 項に記載の情報送信システムにおいて、

上記情報送信装置の上記価格情報作成手段は、上記コンテンツ鍵で暗号化された上記コンテンツデータに付加した上記署名データの検証の有無を表す署名検証情報を格納した上記コンテンツ価格情報を作成し、

上記情報受信装置の上記署名検証手段は、上記コンテンツ価格情報に格納された上記署名検証情報に基づいて、上記コンテンツ鍵で暗号化された上記コンテンツデータに付加した上記署名データを検証するように指定されたときのみ、当該コンテンツ鍵で暗号化された上記コンテンツデータに付加した上記署名データを検証する。

1 2. 請求の範囲第 1 1 項に記載の情報送信システムにおいて、

上記情報送信装置の上記価格情報作成手段は、上記アルバムコンテンツデータに付加した上記署名データの検証の有無を表す上記署名検証情報を格納した上記コンテンツ価格情報を作成し、

上記情報受信装置の上記署名検証手段は、上記コンテンツ価格情報に格納された、上記署名検証情報に基づいて、上記アルバムコンテンツデータに付加した上記署名データを検証するように指定されたときのみ、当該アルバムコンテンツデータに付加した上記署名データを検証する。

1 3. 請求の範囲第 1 2 項に記載の情報送信システムにおいて、

上記情報送信装置の上記取扱方針生成手段は、特定の上記コンテンツデータを取得したときのみ、他の特定の上記コンテンツデータを取得し得るように規定した上記コンテンツ取扱方針を生成する。

1 4. 情報受信装置に所定のコンテンツデータを送信する情報送信装置において

上記情報受信装置固有の所定の配送鍵で暗号化した、上記情報送信装置を識別するための識別情報を保持する識別情報保持手段と、

上記配送鍵で暗号化された上記識別情報と比較するために上記コンテンツデータに上記識別情報を付加する識別情報付加手段と、

上記識別情報を付加した上記コンテンツデータと共に、上記配送鍵で暗号化された上記識別情報を送信する送信手段とを具える。

1 5. 請求の範囲第 1 4 項に記載の情報送信装置において、

上記コンテンツデータに対する使用条件を規定し、上記識別情報を格納したコンテンツ取扱方針を生成する取扱方針生成手段を具え、

上記識別情報付加手段は、上記コンテンツデータに上記コンテンツ取扱方針を付加する。

1 6. 請求の範囲第 1 4 項に記載の情報送信装置において、

上記識別情報付加手段は、上記コンテンツデータに上記識別情報を直接付加する。

1 7. 請求の範囲第 1 4 項に記載の情報送信装置において、

上記コンテンツデータを所定のコンテンツ鍵で暗号化するコンテンツデータ暗号化手段と、

上記コンテンツ鍵を所定の個別鍵で暗号化するコンテンツ鍵暗号化手段と、

上記個別鍵で暗号化した上記コンテンツ鍵及び上記配送鍵で暗号化した上記識別情報に、上記情報受信装置において、不正データ及び改竄をチェックするための署名データを付加する署名付加手段とを具える。

18. 請求の範囲第17項に記載の情報送信装置において、

上記署名付加手段は、上記コンテンツ鍵で暗号化された上記コンテンツデータに上記署名データを付加すると共に、当該署名データを付加した、上記コンテンツ鍵で暗号化された上記コンテンツデータを複数格納してなるアルバムコンテンツデータが生成された際には、当該アルバムコンテンツデータにも上記署名データを付加する。

19. 請求の範囲第18項に記載の情報送信装置において、

上記署名付加手段は、上記個別鍵で暗号化したコンテンツ鍵及び上記配送鍵で暗号化した上記識別情報にそれぞれ上記署名データを付加し、上記アルバムコンテンツデータに対応させて、上記署名データを付加した上記個別鍵で暗号化したコンテンツ鍵及び上記配送鍵で暗号化した上記識別情報を複数格納してアルバム用鍵データが生成された際には、当該アルバム用鍵データにも上記署名データを付加する。

20. 請求の範囲第19項に記載の情報送信装置において、

上記コンテンツデータの使用条件を規定し、上記識別情報を格納したコンテンツ取扱方針を生成する取扱方針生成手段を具え、

上記署名付加手段は、上記コンテンツ取扱方針に上記署名データを付加し、上記アルバムコンテンツデータに対応させて、上記署名データを付加した上記コンテンツ取扱方針を複数格納してアルバム取扱方針が生成された際には、当該アルバム取扱方針にも上記署名データを付加する。

21. 請求の範囲第20項に記載の情報送信装置において、

上記コンテンツデータに対する価格を示すコンテンツ価格情報を作成する価格情報作成手段を具え、

上記署名付加手段は、上記コンテンツ価格情報に上記署名データを付加し、上

記アルバムコンテンツデータに対応させて、上記署名データを付加した上記コンテンツ価格情報を複数格納したアルバム価格情報データが生成された際には、当該アルバム価格情報にも上記署名データを付加する。

22. 請求の範囲第21項に記載の情報送信装置において、

上記取扱方針生成手段は、上記コンテンツ鍵で暗号化された上記コンテンツデータに付加した上記署名データの検証の有無を表す署名検証情報を格納した上記コンテンツ取扱方針を生成する。

23. 請求の範囲第22項に記載の情報送信装置において、

上記取扱方針生成手段は、上記アルバムコンテンツデータに付加した上記署名データの検証の有無を表す上記署名検証情報を格納した上記コンテンツ取扱方針を生成する。

24. 請求の範囲第21項に記載の情報送信装置において、

上記価格情報作成手段は、上記コンテンツ鍵で暗号化された上記コンテンツデータに付加した上記署名データの検証の有無を表す署名検証情報を格納した上記コンテンツ価格情報を作成する。

25. 請求の範囲第24項に記載の情報送信装置において、

上記価格情報作成手段は、上記アルバムコンテンツデータに付加した上記署名データの検証の有無を表す上記署名検証情報を格納した上記コンテンツ価格情報を作成する。

26. 請求の範囲第25項に記載の情報送信装置において、

上記取扱方針生成手段は、特定の上記コンテンツデータを取得したときのみ、他の特定の上記コンテンツデータを取得し得るように規定した上記コンテンツ取

扱方針を生成する。

27. 情報送信装置から送信された所定のコンテンツデータを受信する情報受信装置において、

上記情報受信装置固有の所定の配送鍵を保持する配送鍵保持手段と、

上記情報送信装置から送信された、上記情報送信装置を識別するための識別情報が付加された上記コンテンツデータと、上記配送鍵で暗号化された上記識別情報とを受信する受信手段と、

上記配送鍵で暗号化された上記識別情報を当該配送鍵で復号化する復号化手段と、

上記コンテンツデータに付加された上記識別情報と、上記復号された上記識別情報とを比較する比較手段とを具える。

28. 請求の範囲第27項に記載の情報受信装置において、

上記コンテンツデータに対する購入処理を実行する購入処理手段を具え、

上記受信手段は、上記情報送信装置から送信された上記コンテンツデータと、当該コンテンツデータに付加された上記コンテンツデータに対する使用条件を規定して上記識別情報を格納したコンテンツ取扱方針とを受信し、

上記比較手段は、上記コンテンツ取扱方針に格納された上記識別情報と、復号化された上記識別情報とを比較し、

上記購入処理手段は、上記比較手段において比較した上記識別情報同士が一致したときに、上記コンテンツ取扱方針を用いて上記コンテンツデータの上記購入処理を実行する。

29. 請求の範囲第27項に記載の情報受信装置において、

上記受信手段は、上記情報送信装置から送信された上記コンテンツデータと、当該コンテンツデータに直接付加された上記識別情報とを受信する。

30. 請求の範囲第27項に記載の情報受信装置において、

上記情報送信装置から所定のコンテンツ鍵で暗号化されている上記コンテンツデータと、所定の個別鍵で暗号化されている上記コンテンツ鍵と共に送信された上記個別鍵で暗号化されている上記コンテンツ鍵及び上記配送鍵で暗号化されている上記識別情報に付加された署名データを検証し、上記個別鍵で暗号化されている上記コンテンツ鍵及び上記配送鍵で暗号化されている上記識別情報が不正データ及び改竄されたデータであるか否かを検出する署名検証手段を具える。

31. 請求の範囲第30項に記載の情報受信装置において、

上記署名検証手段は、上記情報送信装置から送信された上記コンテンツ鍵で暗号化されている上記コンテンツデータに付加された上記署名データと、上記コンテンツ鍵で暗号化されている上記コンテンツデータを複数格納してなるアルバムコンテンツデータに付加された上記署名データとのうちの上記アルバムコンテンツデータに付加された上記署名データを検証し、当該検証の結果、上記アルバムコンテンツデータが正しいデータであると判断したときには、当該アルバムコンテンツデータに格納された上記コンテンツ鍵で暗号化されている各上記コンテンツデータに付加された上記署名データの検証を省略する。

32. 請求の範囲第31項に記載の情報受信装置において、

上記署名検証手段は、上記情報送信装置から送信された、上記個別鍵で暗号化されている上記コンテンツ鍵及び上記配送鍵で暗号化されている上記識別情報にそれぞれ付加された上記署名データと、上記アルバムコンテンツデータに対応する上記署名データを付加した上記個別鍵で暗号化されているコンテンツ鍵及び上記配送鍵で暗号化されている上記識別情報を複数格納してなるアルバム用鍵データに付加された上記署名データとのうちの当該アルバム鍵データに付加された上記署名データを検証し、当該検証の結果、上記アルバム鍵データが正しいデータ

であると判断したときには、当該アルバム鍵データに格納された、上記個別鍵で暗号化されている上記コンテンツ鍵及び上記配送鍵で暗号化されている上記識別情報にそれぞれ付加された上記署名データの検証を省略する。

3 3. 請求の範囲第 3 2 項に記載の情報受信装置において、

上記署名検証手段は、上記情報送信装置から送信された、上記コンテンツデータの使用条件を規定して上記識別情報を格納したコンテンツ取扱方針に付加された上記署名データと、上記アルバムコンテンツデータに対応する上記署名データが付加された上記コンテンツ取扱方針を複数格納してなるアルバム取扱方針に付加された上記署名データとのうちの上記アルバム取扱方針に付加された上記署名データを検証し、当該検証の結果、上記アルバム取扱方針が正しいデータであると判断したときには、当該アルバム取扱保身に格納されている上記コンテンツ取扱方針に付加された上記署名データの検証を省略する。

3 4. 請求の範囲第 3 3 項に記載の情報受信装置において、

上記署名検証手段は、上記情報送信装置から送信された、上記コンテンツデータに対する価格を示すコンテンツ価格情報に付加された上記署名データと、上記アルバムコンテンツデータに対応する上記署名データが付加された上記コンテンツ価格情報を複数格納してなるアルバム価格情報データに付加された上記署名データのうちの当該アルバム価格情報に付加された上記署名データを検証し、当該検証の結果、上記アルバム価格情報が正しいデータであると判断したときには、当該アルバム価格情報に格納されている上記コンテンツ価格情報に付加された上記署名データの検証を省略する。

3 5. 請求の範囲第 3 4 項に記載の情報受信装置において、

上記署名検証手段は、上記情報送信装置から送信された、上記コンテンツ鍵で暗号化されている上記コンテンツデータと、当該コンテンツ鍵で暗号化されてい



る上記コンテンツデータに付加された上記署名データと、当該署名データの検証の有無を表す署名検証情報が格納された上記コンテンツ取扱方針との中の当該コンテンツ取扱方針に格納された上記署名検証情報に基づいて上記署名データを検証するように指定されたときのみ、上記コンテンツ鍵で暗号化されている上記コンテンツデータに付加された上記署名データを検証する。

36. 請求の範囲第35項に記載の情報受信装置において、

上記署名検証手段は、上記情報送信装置から送信された上記アルバムコンテンツデータと、当該アルバムコンテンツデータに付加された上記署名データと、当該署名データの検証の有無を表す上記署名検証情報が格納された上記コンテンツ取扱方針との中の当該コンテンツ取扱方針に格納された上記署名検証情報に基づいて上記署名データを検証するように指定されたときのみ、当該アルバムコンテンツデータに付加された上記署名データを検証する。

37. 請求の範囲第34項に記載の情報受信装置において、

上記署名検証手段は、上記情報送信装置から送信された、上記コンテンツ鍵で暗号化されている上記コンテンツデータと、当該コンテンツ鍵で暗号化されている上記コンテンツデータに付加された上記署名データと、当該署名データの検証の有無を表す署名検証情報が格納された上記コンテンツ価格情報との中の当該コンテンツ価格情報に格納された上記署名検証情報に基づいて上記署名データを検証するように指定されたときのみ、上記コンテンツ鍵で暗号化されている上記コンテンツデータに付加された上記署名データを検証する。

38. 請求の範囲第37項に記載の情報受信装置において、

上記署名検証手段は、上記情報送信装置から送信された上記アルバムコンテンツデータと、当該アルバムコンテンツデータに付加された上記署名データと、当該署名データの検証の有無を表す上記署名検証情報が格納された上記コンテンツ

価格情報との中の当該コンテンツ価格情報に格納された上記署名検証情報に基づいて上記署名データを検証するように指定されたときのみ、上記アルバムコンテンツデータに付加された上記署名データを検証する。

39. 請求の範囲第38項に記載の情報受信装置において、

上記受信手段は、特定の上記コンテンツデータを取得したときのみ、他の特定の上記コンテンツデータを取得し得るように規定した上記コンテンツ取扱方針を受信する。

40. 情報送信装置から所定のコンテンツデータを情報受信装置に送信する情報送信方法において、

上記情報送信装置により、上記コンテンツデータに当該情報送信装置を識別するための識別情報を付加する識別情報付加ステップと、

上記情報送信装置により、上記識別情報を付加したコンテンツデータと、上記情報受信装置固有の配送鍵で暗号化した、上記情報送信装置を識別するための識別情報とを送信する送信ステップと、

上記情報受信装置により、上記識別情報が付加された上記コンテンツデータ及び上記配送鍵で暗号化された上記識別情報を受信する受信ステップと、

上記情報受信装置により、上記配送鍵で暗号化された上記識別情報を当該配送鍵で復号化する復号化ステップと、

上記情報受信装置により、上記コンテンツデータに付加された上記識別情報と、上記復号された上記識別情報とを比較する比較ステップとを具える。

41. 請求の範囲第40項に記載の情報送信方法において、

上記情報送信装置により、上記コンテンツデータに対する使用条件を規定し、上記識別情報を格納したコンテンツ取扱方針を生成する取扱方針生成ステップと

上記コンテンツデータに上記コンテンツ取扱方針を付加する取扱方針付加ステップとを具える。

4 2. 請求の範囲第 4 0 項に記載の情報送信方法において、

上記識別情報付加ステップは、上記コンテンツデータに上記識別情報を直接付加する。

4 3. 請求の範囲第 4 0 項に記載の情報送信方法において、

上記情報送信装置により、上記コンテンツデータを所定のコンテンツ鍵で暗号化するコンテンツデータ暗号化ステップと、

上記情報送信装置により、上記コンテンツ鍵を所定の個別鍵で暗号化するコンテンツ鍵暗号化ステップと、

上記情報送信装置により、上記個別鍵で暗号化したコンテンツ鍵及び上記配送鍵で暗号化した識別情報に、不正データ及び改竄をチェックするための署名データを付加する署名付加ステップと、

上記情報受信装置により、上記個別鍵で暗号化したコンテンツ鍵及び上記配送鍵で暗号化した識別情報に付加された上記署名データを検証する署名検証ステップとを具える。

4 4. 請求の範囲第 4 3 項に記載の情報送信方法において、

上記署名付加ステップは、上記コンテンツ鍵で暗号化された上記コンテンツデータに上記署名データを付加すると共に、当該署名データを付加した、上記コンテンツ鍵で暗号化された上記コンテンツデータを複数格納してなるアルバムコンテンツデータが生成された際には、当該アルバムコンテンツデータにも上記署名データを付加し、

上記署名検証ステップは、上記アルバムコンテンツデータに付加された上記署名データを検証し、当該検証の結果、上記アルバムコンテンツデータが正しいデ

ータであると判断したときには、当該アルバムコンテンツデータに格納された上記コンテンツ鍵で暗号化された各上記コンテンツデータに付加された上記署名データの検証を省略する。

45. 請求の範囲第44項に記載の情報送信方法において、

上記署名付加ステップは、上記個別鍵で暗号化したコンテンツ鍵及び上記配送鍵で暗号化した上記識別情報にそれぞれ上記署名データを付加し、上記アルバムコンテンツデータに対応させて、上記署名データを付加した上記個別鍵で暗号化したコンテンツ鍵及び上記配送鍵で暗号化した上記識別情報を複数格納してアルバム用鍵データが生成された際には、当該アルバム用鍵データにも上記署名データを付加し、

上記署名検証ステップは、上記アルバム鍵データに付加された上記署名データを検証し、当該検証の結果、上記アルバム鍵データが正しいデータであると判断したときには、当該アルバム鍵データに格納された、上記個別鍵で暗号化したコンテンツ鍵及び上記配送鍵で暗号化した上記識別情報にそれぞれ付加された上記署名データの検証を省略する。

46. 請求の範囲第45項に記載の情報送信方法において、

上記コンテンツデータの使用条件を規定し、上記識別情報を格納したコンテンツ取扱方針を生成する取扱方針生成ステップを具え、

上記署名付加ステップは、上記コンテンツ取扱方針に上記署名データを付加し、上記アルバムコンテンツデータに対応させて、上記署名データを付加した上記コンテンツ取扱方針を複数格納してアルバム取扱方針が生成された際には、当該アルバム取扱方針にも上記署名データを付加し、

上記署名検証ステップは、上記アルバム取扱方針に付加された上記署名データを検証し、当該検証の結果、上記アルバム取扱方針が正しいデータであると判断したときには、当該アルバム取扱保身に格納された上記コンテンツ取扱方針に付

加された上記署名データの検証を省略する。

47. 請求の範囲第46項に記載の情報送信方法において、

上記コンテンツデータに対する価格を示すコンテンツ価格情報を作成する価格情報作成ステップを具え、

上記署名付加ステップは、上記コンテンツ価格情報に上記署名データを付加し、上記アルバムコンテンツデータに対応させて、上記署名データを付加した上記コンテンツ価格情報を複数格納したアルバム価格情報データが生成された際には、当該アルバム価格情報にも上記署名データを付加し、

上記署名検証ステップは、上記アルバム価格情報に付加された上記署名データを検証し、当該検証の結果、上記アルバム価格情報が正しいデータであると判断したときには、当該アルバム価格情報に格納された上記コンテンツ価格情報に付加された上記署名データの検証を省略する。

48. 請求の範囲第47項に記載の情報送信方法において、

上記取扱方針生成ステップは、上記コンテンツ鍵で暗号化された上記コンテンツデータに付加した上記署名データの検証の有無を表す署名検証情報を格納した上記コンテンツ取扱方針を生成し、

上記署名検証ステップは、上記コンテンツ取扱方針に格納された、上記署名検証情報に基づいて、上記コンテンツ鍵で暗号化された上記コンテンツデータに付加した上記署名データを検証するように指定されたときのみ、当該コンテンツ鍵で暗号化された上記コンテンツデータに付加した上記署名データを検証する。

49. 請求の範囲第48項に記載の情報送信方法において、

上記取扱方針生成ステップは、上記アルバムコンテンツデータに付加した上記署名データの検証の有無を表す上記署名検証情報を格納した上記コンテンツ取扱方針を生成し、

上記署名検証ステップは、上記コンテンツ取扱方針に格納された、上記署名検証情報に基づいて、上記アルバムコンテンツデータに付加した上記署名データを検証するように指定されたときのみ、当該アルバムコンテンツデータに付加した上記署名データを検証する。

50. 請求の範囲第47項に記載の情報送信方法において、

上記価格情報作成ステップは、上記コンテンツ鍵で暗号化された上記コンテンツデータに付加した上記署名データの検証の有無を表す署名検証情報を格納した上記コンテンツ価格情報を作成し、

上記署名検証ステップは、上記コンテンツ価格情報に格納された、上記署名検証情報に基づいて、上記コンテンツ鍵で暗号化された上記コンテンツデータに付加した上記署名データを検証するように指定されたときのみ、当該コンテンツ鍵で暗号化された上記コンテンツデータに付加した上記署名データを検証する。

51. 請求の範囲第50項に記載の情報送信方法において、

上記価格情報作成ステップは、上記アルバムコンテンツデータに付加した上記署名データの検証の有無を表す上記署名検証情報を格納した上記コンテンツ価格情報を作成し、

上記署名検証ステップは、上記コンテンツ価格情報に格納された、上記署名検証情報に基づいて、上記アルバムコンテンツデータに付加した上記署名データを検証するように指定されたときのみ、当該アルバムコンテンツデータに付加した上記署名データを検証する。

52. 請求の範囲第51項に記載の情報送信方法において、

上記取扱方針生成ステップは、特定の上記コンテンツデータを取得したときのみ、他の特定の上記コンテンツデータを取得し得るように規定した上記コンテンツ取扱方針を生成する。

### 5 3. 情報受信装置に所定のコンテンツデータを送信する情報送信方法において

上記情報受信装置固有の所定の配送鍵で暗号化して予め保持している上記情報送信装置を識別するための識別情報と比較するために上記コンテンツデータに上記識別情報を付加する識別情報付加ステップと、

上記識別情報を付加した上記コンテンツデータと共に、上記配送鍵で暗号化された上記識別情報を上記情報受信装置に送信する送信ステップとを具える。

### 5 4. 請求の範囲第 5 3 項に記載の情報送信方法において、

上記コンテンツデータに対する使用条件を規定し、上記識別情報を格納したコンテンツ取扱方針を生成する取扱方針生成ステップと、

上記コンテンツデータに上記コンテンツ取扱方針を付加する取扱方針付加ステップとを具える。

### 5 5. 請求の範囲第 5 3 項に記載の情報送信方法において、

上記識別情報付加ステップは、上記コンテンツデータに上記識別情報を直接付加する。

### 5 6. 請求の範囲第 5 3 項に記載の情報送信方法において、

上記コンテンツデータを所定のコンテンツ鍵で暗号化するコンテンツデータ暗号化ステップと、

上記コンテンツ鍵を所定の個別鍵で暗号化するコンテンツ鍵暗号化ステップと

上記個別鍵で暗号化した上記コンテンツ鍵及び上記配送鍵で暗号化した上記識別情報に、上記情報受信装置において、不正データ及び改竄をチェックするための署名データを付加する署名付加ステップとを具える。

57. 請求の範囲第56項に記載の情報送信方法において、

上記署名付加ステップは、上記コンテンツ鍵で暗号化された上記コンテンツデータに上記署名データを付加すると共に、当該署名データを付加した、上記コンテンツ鍵で暗号化された上記コンテンツデータを複数格納してなるアルバムコンテンツデータが生成された際には、当該アルバムコンテンツデータにも上記署名データを付加する。

58. 請求の範囲第57項に記載の情報送信方法において、

上記署名付加ステップは、上記個別鍵で暗号化したコンテンツ鍵及び上記配送鍵で暗号化した上記識別情報にそれぞれ上記署名データを付加し、上記アルバムコンテンツデータに対応させて、上記署名データを付加した上記個別鍵で暗号化したコンテンツ鍵及び上記配送鍵で暗号化した上記識別情報を複数格納してアルバム用鍵データが生成された際には、当該アルバム用鍵データにも上記署名データを付加する。

59. 請求の範囲第58項に記載の情報送信方法において、

上記コンテンツデータの使用条件を規定し、上記識別情報を格納したコンテンツ取扱方針を生成する取扱方針生成ステップを具え、

上記署名付加ステップは、上記コンテンツ取扱方針に上記署名データを付加し、上記アルバムコンテンツデータに対応させて、上記署名データを付加した上記コンテンツ取扱方針を複数格納してアルバム取扱方針が生成された際には、当該アルバム取扱方針にも上記署名データを付加する。

60. 請求の範囲第59項に記載の情報送信方法において、

上記コンテンツデータに対する価格を示すコンテンツ価格情報を作成する価格情報作成ステップを具え、

上記署名付加ステップは、上記コンテンツ価格情報に上記署名データを付加し



、上記アルバムコンテンツデータに対応させて、上記署名データを付加した上記コンテンツ価格情報を複数格納したアルバム価格情報データが生成された際には、当該アルバム価格情報にも上記署名データを付加する。

6 1. 請求の範囲第 6 0 項に記載の情報送信方法において、

上記取扱方針生成ステップは、上記コンテンツ鍵で暗号化された上記コンテンツデータに付加した上記署名データの検証の有無を表す署名検証情報を格納した上記コンテンツ取扱方針を生成する。

6 2. 請求の範囲第 6 1 項に記載の情報送信方法において、

上記取扱方針生成ステップは、上記アルバムコンテンツデータに付加した上記署名データの検証の有無を表す上記署名検証情報を格納した上記コンテンツ取扱方針を生成する。

6 3. 請求の範囲第 6 0 項に記載の情報送信方法において、

上記価格情報作成ステップは、上記コンテンツ鍵で暗号化された上記コンテンツデータに付加した上記署名データの検証の有無を表す署名検証情報を格納した上記コンテンツ価格情報を作成する。

6 4. 請求の範囲第 6 3 項に記載の情報送信方法において、

上記価格情報作成ステップは、上記アルバムコンテンツデータに付加した上記署名データの検証の有無を表す上記署名検証情報を格納した上記コンテンツ価格情報を作成する。

6 5. 請求の範囲第 6 4 項に記載の情報送信方法において、

上記取扱方針生成ステップは、特定の上記コンテンツデータを取得したときの、他の特定の上記コンテンツデータを取得し得るように規定した上記コンテ

ツ取扱方針を生成する。

66. 情報送信装置から送信された所定のコンテンツデータを受信する情報受信方法において、

上記情報送信装置から送信された、上記情報送信装置を識別するための識別情報が付加された上記コンテンツデータと、上記情報受信装置固有の所定の配送鍵で暗号化された上記識別情報とを受信する受信ステップと、

上記配送鍵で暗号化された上記識別情報を当該配送鍵で復号化する復号化ステップと、

上記コンテンツデータに付加された上記識別情報と、上記復号された上記識別情報とを比較する比較ステップとを具える。

67. 請求の範囲第66項に記載の情報受信方法において、

上記コンテンツデータに対する購入処理を実行する購入処理ステップを具え、

上記受信ステップは、上記情報送信装置から送信された上記コンテンツデータと、当該コンテンツデータに付加された当該コンテンツデータに対する使用条件を規定して上記識別情報を格納したコンテンツ取扱方針とを受信し、

比較ステップは、上記コンテンツ取扱方針に格納された上記識別情報と、復号化された上記識別情報とを比較し、

上記購入処理ステップは、上記比較ステップにおいて比較した上記識別情報同士が一致したときに、上記コンテンツ取扱方針を用いて上記コンテンツデータの上記購入処理を実行する。

68. 請求の範囲第66項に記載の情報受信方法において、

上記比較ステップは、上記コンテンツデータに直接付加された上記識別情報と、上記復号された上記識別情報とを比較する。

69. 請求の範囲第66項に記載の情報受信方法において、

上記情報送信装置から所定のコンテンツ鍵で暗号化されている上記コンテンツデータと、所定の個別鍵で暗号化されている上記コンテンツ鍵と共に送信された上記個別鍵で暗号化されている上記コンテンツ鍵及び上記配送鍵で暗号化されている上記識別情報に付加された署名データを検証し、上記個別鍵で暗号化されている上記コンテンツ鍵及び上記配送鍵で暗号化されている上記識別情報が不正データ及び改竄されたデータであるか否かを検出する署名検証ステップを具える。

70. 請求の範囲第69項に記載の情報受信方法において、

上記署名検証ステップは、上記情報送信装置から送信された上記コンテンツ鍵で暗号化されている上記コンテンツデータに付加された上記署名データと、上記コンテンツ鍵で暗号化されている上記コンテンツデータを複数格納してなるアルバムコンテンツデータに付加された上記署名データとのうちの当該アルバムコンテンツデータに付加された上記署名データを検証し、当該検証の結果、上記アルバムコンテンツデータが正しいデータであると判断したときには、当該アルバムコンテンツデータに格納された上記コンテンツ鍵で暗号化されている各上記コンテンツデータに付加された上記署名データの検証を省略する。

71. 請求の範囲第70項に記載の情報受信方法において、

上記署名検証ステップは、上記情報送信装置から送信された上記個別鍵で暗号化されている上記コンテンツ鍵及び上記配送鍵で暗号化されている上記識別情報にそれぞれ付加された上記署名データと、上記アルバムコンテンツデータに対応する上記個別鍵で暗号化されているコンテンツ鍵及び上記配送鍵で暗号化されている上記識別情報を複数格納してなるアルバム用鍵データに付加された上記署名データとのうちの当該アルバム鍵データに付加された上記署名データを検証し、当該検証の結果、上記アルバム鍵データが正しいデータであると判断したときには、当該アルバム鍵データに格納された上記個別鍵で暗号化されているコンテン

ツ鍵及び上記配送鍵で暗号化されている上記識別情報にそれぞれ付加された上記署名データの検証を省略する。

7 2. 請求の範囲第 7 1 項に記載の情報受信方法において、

上記署名検証ステップは、上記情報送信装置から送信された上記コンテンツデータの使用条件を規定して上記識別情報を格納したコンテンツ取扱方針に付加された上記署名データと、上記アルバムコンテンツデータに対応する上記コンテンツ取扱方針を複数格納してなるアルバム取扱方針に付加された上記署名データとのうちの当該アルバム取扱方針に付加された上記署名データを検証し、当該検証の結果、上記アルバム取扱方針が正しいデータであると判断したときには、当該アルバム取扱保身に格納されている上記コンテンツ取扱方針に付加された上記署名データの検証を省略する。

7 3. 請求の範囲第 7 2 項に記載の情報受信方法において、

上記署名検証ステップは、上記情報送信装置から送信された上記コンテンツデータに対する価格を示すコンテンツ価格情報に付加された上記署名データと、上記アルバムコンテンツデータに対応する上記コンテンツ価格情報を複数格納してなるアルバム価格情報データに付加された上記署名データとのうちの当該アルバム価格情報に付加された上記署名データを検証し、当該検証の結果、上記アルバム価格情報が正しいデータであると判断したときには、当該アルバム価格情報に格納されている上記コンテンツ価格情報に付加された上記署名データの検証を省略する。

7 4. 請求の範囲第 7 3 項に記載の情報受信方法において、

上記署名検証ステップは、上記情報送信装置から送信された上記コンテンツ鍵で暗号化されている上記コンテンツデータと、当該コンテンツ鍵で暗号化されている上記コンテンツデータに付加された上記署名データと、当該署名データの検

証の有無を表す署名検証情報を格納した上記コンテンツ取扱方針との中の当該コンテンツ取扱方針に格納された上記署名検証情報に基づいて上記署名データを検証するように指定されたときのみ、上記コンテンツ鍵で暗号化されている上記コンテンツデータに付加された上記署名データを検証する。

75. 請求の範囲第74項に記載の情報受信方法において、

上記署名検証ステップは、上記情報送信装置から送信された上記アルバムコンテンツデータと、当該アルバムコンテンツデータに付加された上記署名データと、当該署名データの検証の有無を表す上記署名検証情報を格納した上記コンテンツ取扱方針との中の当該コンテンツ取扱方針に格納された上記署名検証情報に基づいて上記署名データを検証するように指定されたときのみ、上記アルバムコンテンツデータに付加された上記署名データを検証する。

76. 請求の範囲第73項に記載の情報受信方法において、

上記署名検証ステップは、上記情報送信装置から送信された上記コンテンツ鍵で暗号化されている上記コンテンツデータと、当該コンテンツ鍵で暗号化されている上記コンテンツデータに付加された上記署名データと、当該署名データの検証の有無を表す署名検証情報を格納した上記コンテンツ価格情報との中の当該コンテンツ価格情報に格納された上記署名検証情報に基づいて上記署名データを検証するように指定されたときのみ、上記コンテンツ鍵で暗号化されている上記コンテンツデータに付加された上記署名データを検証する。

77. 請求の範囲第76項に記載の情報受信方法において、

上記署名検証ステップは、上記情報送信装置から送信された上記アルバムコンテンツデータと、当該アルバムコンテンツデータに付加された上記署名データと、当該署名データの検証の有無を表す上記署名検証情報を格納した上記コンテンツ価格情報との中の当該コンテンツ価格情報に格納された上記署名検証情報に

基づいて上記署名データを検証するように指定されたときのみ、上記アルバムコンテンツデータに付加された上記署名データを検証する。

78. 請求の範囲第77項に記載の情報受信方法において、

上記受信ステップは、特定の上記コンテンツデータを取得したときのみ、他の特定の上記コンテンツデータを取得し得るように規定した上記コンテンツ取扱方針を受信する。

79. 所定のプログラムを格納し、当該プログラムを情報送信装置に供給するプログラム格納媒体において、

上記プログラムは、

上記情報受信装置固有の所定の配送鍵で暗号化して予め保持している上記情報送信装置を識別するための識別情報と比較するために上記コンテンツデータに上記識別情報を付加する識別情報付加ステップと、

上記識別情報を付加した上記コンテンツデータと共に、上記配送鍵で暗号化された上記識別情報を上記情報受信装置に送信する送信ステップとを具える。

80. 請求の範囲第79項に記載のプログラム格納媒体において、

上記プログラムは、

上記コンテンツデータに対する使用条件を規定し、上記識別情報を格納したコンテンツ取扱方針を生成する取扱方針生成ステップと、

上記コンテンツデータに上記コンテンツ取扱方針を付加する取扱方針付加ステップとを具える。

81. 請求の範囲第79項に記載のプログラム格納媒体において、

上記プログラムの上記識別情報付加ステップは、上記コンテンツデータに上記識別情報を直接付加する。

82. 請求の範囲第79項に記載のプログラム格納媒体において、

上記プログラムは、

上記コンテンツデータを所定のコンテンツ鍵で暗号化するコンテンツデータ暗号化ステップと、

上記コンテンツ鍵を所定の個別鍵で暗号化するコンテンツ鍵暗号化ステップと

、  
上記個別鍵で暗号化した上記コンテンツ鍵及び上記配送鍵で暗号化した上記識別情報に、上記情報受信装置において、不正データ及び改竄をチェックするための署名データを付加する署名付加ステップとを具える。

83. 請求の範囲第82項に記載のプログラム格納媒体において、

上記プログラムの上記署名付加ステップは、上記コンテンツ鍵で暗号化された上記コンテンツデータに上記署名データを付加すると共に、当該署名データを付加した、上記コンテンツ鍵で暗号化された上記コンテンツデータを複数格納してなるアルバムコンテンツデータが生成された際には、当該アルバムコンテンツデータにも上記署名データを付加する。

84. 請求の範囲第83項に記載のプログラム格納媒体において、

上記プログラムの上記署名付加ステップは、上記個別鍵で暗号化したコンテンツ鍵及び上記配送鍵で暗号化した上記識別情報にそれぞれ上記署名データを付加し、上記アルバムコンテンツデータに対応させて、上記署名データを付加した上記個別鍵で暗号化したコンテンツ鍵及び上記配送鍵で暗号化した上記識別情報を複数格納してアルバム用鍵データが生成された際には、当該アルバム用鍵データにも上記署名データを付加する。

85. 請求の範囲第84項に記載のプログラム格納媒体において、

上記プログラムは、

上記コンテンツデータの使用条件を規定し、上記識別情報を格納したコンテンツ取扱方針を生成する取扱方針生成ステップを具え、

上記署名付加ステップは、上記コンテンツ取扱方針に上記署名データを付加し、上記アルバムコンテンツデータに対応させて、上記署名データを付加した上記コンテンツ取扱方針を複数格納してアルバム取扱方針が生成された際には、当該アルバム取扱方針にも上記署名データを付加する。

86. 請求の範囲第85項に記載のプログラム格納媒体において、

上記プログラムは、

上記コンテンツデータに対する価格を示すコンテンツ価格情報を作成する価格情報作成ステップを具え、

上記署名付加ステップは、上記コンテンツ価格情報に上記署名データを付加し、上記アルバムコンテンツデータに対応させて、上記署名データを付加した上記コンテンツ価格情報を複数格納したアルバム価格情報データが生成された際には、当該アルバム価格情報にも上記署名データを付加する。

87. 請求の範囲第86項に記載のプログラム格納媒体において、

上記プログラムの上記取扱方針生成ステップは、上記コンテンツ鍵で暗号化された上記コンテンツデータに付加した上記署名データの検証の有無を表す署名検証情報を格納した上記コンテンツ取扱方針を生成する。

88. 請求の範囲第87項に記載のプログラム格納媒体において、

上記プログラムの上記取扱方針生成ステップは、上記アルバムコンテンツデータに付加した上記署名データの検証の有無を表す上記署名検証情報を格納した上記コンテンツ取扱方針を生成する。

89. 請求の範囲第86項に記載のプログラム格納媒体において、



上記プログラムの上記価格情報作成ステップは、上記コンテンツ鍵で暗号化された上記コンテンツデータに付加した上記署名データの検証の有無を表す署名検証情報を格納した上記コンテンツ価格情報を作成する。

90. 請求の範囲第89項に記載のプログラム格納媒体において、

上記プログラムの上記価格情報作成ステップは、上記アルバムコンテンツデータに付加した上記署名データの検証の有無を表す上記署名検証情報を格納した上記コンテンツ価格情報を作成する。

91. 請求の範囲第90項に記載のプログラム格納媒体において、

上記プログラムの上記取扱方針生成ステップは、特定の上記コンテンツデータを取得したときのみ、他の特定の上記コンテンツデータを取得し得るように規定した上記コンテンツ取扱方針を生成する。

92. 所定のプログラムを格納し、当該プログラムを情報受信装置に供給するプログラム格納媒体において、

上記プログラムは

情報送信装置から送信された、上記情報送信装置を識別するための識別情報が付加された所定のコンテンツデータと、情報受信装置固有の所定の配送鍵で暗号化された上記識別情報とを受信する受信ステップと、

上記配送鍵で暗号化された上記識別情報を当該配送鍵で復号化する復号化ステップと、

上記コンテンツデータに付加された上記識別情報と、上記復号された上記識別情報とを比較する比較ステップとを具える。

93. 請求の範囲第92項に記載のプログラム格納媒体において、

上記プログラムは、

上記コンテンツデータに対する購入処理を実行する購入処理ステップを具え、  
上記受信ステップは、上記情報送信装置から送信された上記コンテンツデータ  
と、当該コンテンツデータに付加された当該コンテンツデータに対する使用条件  
を規定して上記識別情報を格納したコンテンツ取扱方針とを受信し、

比較ステップは、上記コンテンツ取扱方針に格納された上記識別情報と、復号  
化された上記識別情報とを比較し、

上記購入処理ステップは、上記比較ステップにおいて比較した上記識別情報同  
士が一致したときに、上記コンテンツ取扱方針を用いて上記コンテンツデータの  
上記購入処理を実行する。

9 4. 請求の範囲第 9 2 項に記載のプログラム格納媒体において、

上記プログラムの上記比較ステップは、上記コンテンツデータに直接付加され  
た上記識別情報と、上記復号された上記識別情報とを比較する。

9 5. 請求の範囲第 9 2 項に記載のプログラム格納媒体において、

上記プログラムは、

上記情報送信装置から所定のコンテンツ鍵で暗号化されている上記コンテンツ  
データと、所定の個別鍵で暗号化されている上記コンテンツ鍵と共に送信された  
上記個別鍵で暗号化されている上記コンテンツ鍵及び上記配送鍵で暗号化されて  
いる上記識別情報に付加された署名データを検証し、上記個別鍵で暗号化されて  
いる上記コンテンツ鍵及び上記配送鍵で暗号化されている上記識別情報が不正デ  
ータ及び改竄されたデータであるか否かを検出する署名検証ステップを具える。

9 6. 請求の範囲第 9 5 項に記載のプログラム格納媒体において、

上記プログラムの上記署名検証ステップは、上記情報送信装置から送信された  
上記コンテンツ鍵で暗号化されている上記コンテンツデータに付加された上記署  
名データと、上記コンテンツ鍵で暗号化されている上記コンテンツデータを複数

格納してなるアルバムコンテンツデータに付加された上記署名データとの中の当該アルバムコンテンツデータに付加された上記署名データを検証し、当該検証の結果、上記アルバムコンテンツデータが正しいデータであると判断したときには、当該アルバムコンテンツデータに格納された上記コンテンツ鍵で暗号化されている各上記コンテンツデータに付加された上記署名データの検証を省略する。

97. 請求の範囲第96項に記載のプログラム格納媒体において、

上記プログラムの上記署名検証ステップは、上記情報送信装置から送信された上記個別鍵で暗号化されている上記コンテンツ鍵及び上記配送鍵で暗号化されている上記識別情報にそれぞれ付加された上記署名データと、上記アルバムコンテンツデータに対応する上記個別鍵で暗号化されているコンテンツ鍵及び上記配送鍵で暗号化されている上記識別情報を複数格納してなるアルバム用鍵データに付加された上記署名データとの中の当該アルバム鍵データに付加された上記署名データを検証し、当該検証の結果、上記アルバム鍵データが正しいデータであると判断したときには、当該アルバム鍵データに格納された上記個別鍵で暗号化されているコンテンツ鍵及び上記配送鍵で暗号化されている上記識別情報にそれぞれ付加された上記署名データの検証を省略する。

98. 請求の範囲第97項に記載のプログラム格納媒体において、

上記プログラムの上記署名検証ステップは、上記情報送信装置から送信された上記コンテンツデータの使用条件を規定して上記識別情報を格納したコンテンツ取扱方針に付加された上記署名データと、上記アルバムコンテンツデータに対応する上記コンテンツ取扱方針を複数格納してなるアルバム取扱方針に付加された上記署名データとの中の当該アルバム取扱方針に付加された上記署名データを検証し、当該検証の結果、上記アルバム取扱方針が正しいデータであると判断したときには、当該アルバム取扱保身に格納されている上記コンテンツ取扱方針に付加された上記署名データの検証を省略する。

99. 請求の範囲第98項に記載のプログラム格納媒体において、

上記プログラムの上記署名検証ステップは、上記情報送信装置から送信された上記コンテンツデータに対する価格を示すコンテンツ価格情報に付加された上記署名データと、上記アルバムコンテンツデータに対応する上記コンテンツ価格情報を複数格納してなるアルバム価格情報データに付加された上記署名データとのうちの当該アルバム価格情報に付加された上記署名データを検証し、当該検証の結果、上記アルバム価格情報が正しいデータであると判断したときには、当該アルバム価格情報に格納されている上記コンテンツ価格情報に付加された上記署名データの検証を省略する。

100. 請求の範囲第99項に記載のプログラム格納媒体において、

上記プログラムの上記署名検証ステップは、上記情報送信装置から送信された上記コンテンツ鍵で暗号化されている上記コンテンツデータと、当該コンテンツ鍵で暗号化されている上記コンテンツデータに付加された上記署名データと、当該署名データの検証の有無を表す署名検証情報を格納した上記コンテンツ取扱方針とのうちの当該コンテンツ取扱方針に格納された上記署名検証情報に基づいて上記署名データを検証するように指定されたときのみ、上記コンテンツ鍵で暗号化されている上記コンテンツデータに付加された上記署名データを検証する。

101. 請求の範囲第100項に記載のプログラム格納媒体において、

上記プログラムの上記署名検証ステップは、上記情報送信装置から送信された上記アルバムコンテンツデータと、当該アルバムコンテンツデータに付加された上記署名データと、当該署名データの検証の有無を表す上記署名検証情報を格納した上記コンテンツ取扱方針とのうちの当該コンテンツ取扱方針に格納された上記署名検証情報に基づいて上記署名データを検証するように指定されたときのみ、当該アルバムコンテンツデータに付加された上記署名データを検証する。

102. 請求の範囲第99項に記載のプログラム格納媒体において、

上記プログラムの上記署名検証ステップは、上記情報送信装置から送信された上記コンテンツ鍵で暗号化されている上記コンテンツデータと、当該コンテンツ鍵で暗号化されている上記コンテンツデータに付加された上記署名データと、当該署名データの検証の有無を表す署名検証情報を格納した上記コンテンツ価格情報とのうちの当該コンテンツ価格情報に格納された上記署名検証情報に基づいて上記署名データを検証するように指定されたときのみ、当該コンテンツ鍵で暗号化されている上記コンテンツデータに付加された上記署名データを検証する。

103. 請求の範囲第102項に記載のプログラム格納媒体において、

上記プログラムの上記署名検証ステップは、上記情報送信装置から送信された上記アルバムコンテンツデータと、当該アルバムコンテンツデータに付加された上記署名データと、当該署名データの検証の有無を表す上記署名検証情報を格納した上記コンテンツ価格情報とのうちの当該コンテンツ価格情報に格納された上記署名検証情報に基づいて上記署名データを検証するように指定されたときのみ、当該アルバムコンテンツデータに付加された上記署名データを検証する。

104. 請求の範囲第103項に記載のプログラム格納媒体において、

上記プログラムの上記受信ステップは、特定の上記コンテンツデータを取得したときのみ、他の特定の上記コンテンツデータを取得し得るように規定した上記コンテンツ取扱方針を受信する。

105. 情報送信装置から所定のコンテンツデータを情報受信装置に送信する情報送信システムにおいて、

上記情報送信装置は、

上記コンテンツデータと共に、当該コンテンツデータに対して、予め規定した再送信可能な最大回数データを送信する送信手段を具え、

上記情報受信装置は、  
上記コンテンツデータと共に、上記最大回数データを受信する受信手段と、  
上記最大回数データに基づいて、上記コンテンツデータの再送信可能な残り回数データを生成する回数データ生成手段と、  
上記コンテンツデータと共に、上記残り回数データを送信する再送信手段とを  
具える。

106. 請求の範囲第105項に記載の情報送信システムにおいて、

上記情報受信装置の上記回数データ生成手段は、上記コンテンツデータの供給元に基づいて、当該コンテンツデータが経由した装置を示す経由装置データを生成し、

上記再送信手段は、上記コンテンツデータ及び上記残り回数データと共に、上記経由装置データを送信する。

107. 所定のコンテンツデータを情報受信装置に送信する情報送信装置において、

上記コンテンツデータと共に、当該コンテンツデータに対して、予め規定した再送信可能な最大回数データを上記情報受信装置に送信する送信手段を具える。

108. 情報送信装置から送信される所定のコンテンツデータを受信する情報受信装置において、

上記情報送信装置から送信された、上記コンテンツデータと、当該コンテンツデータに対して予め規定した再送信可能な最大回数データとを受信する受信手段と、

上記最大回数データに基づいて、上記コンテンツデータの再送信可能な残り回数データを生成する回数データ生成手段と、

上記コンテンツデータと共に、上記残り回数データを送信する再送信手段とを

具える。

109. 請求の範囲第108項に記載の情報受信装置において、

上記回数データ生成手段は、上記コンテンツデータの供給元に基づいて、当該コンテンツデータが経由した装置を示す経由装置データを生成し、

上記再送信手段は、上記コンテンツデータ及び上記残り回数データと共に、上記経由装置データを送信する。

110. 情報送信装置から所定のコンテンツデータを情報受信装置に送信する情報送信方法において、

上記情報送信装置により、上記コンテンツデータと共に、当該コンテンツデータに対して、予め規定した再送信可能な最大回数データを送信する送信ステップと、

上記情報受信装置により、上記コンテンツデータと共に、上記最大回数データを受信する受信ステップと、

上記情報受信装置により、上記最大回数データに基づいて、上記コンテンツデータの再送信可能な残り回数データを生成する回数データ生成ステップと、

上記情報受信装置により、上記コンテンツデータと共に、上記残り回数データを送信する再送信ステップとを具える。

111. 請求の範囲第110項に記載の情報送信方法において、

上記回数データ生成ステップは、上記コンテンツデータの供給元に基づいて、当該コンテンツデータが経由した装置を示す経由装置データを生成し、

上記再送信ステップは、上記コンテンツデータ及び上記残り回数データと共に、上記経由装置データを送信する。

112. 所定のコンテンツデータを情報受信装置に送信する情報送信方法におい

て、

上記コンテンツデータと共に、当該コンテンツデータに対して予め規定した再送信可能な最大回数データを上記情報受信装置に送信する送信ステップを具える。

113. 情報送信装置から送信される所定のコンテンツデータを受信する情報受信方法において、

上記情報送信装置から送信された、上記コンテンツデータと、当該コンテンツデータに対して予め規定した再送信可能な最大回数データとを受信する受信ステップと、

上記最大回数データに基づいて、上記コンテンツデータの再送信可能な残り回数データを生成する回数データ生成ステップと、

上記コンテンツデータと共に、上記残り回数データを送信する再送信ステップとを具える。

114. 請求の範囲第113項に記載の情報受信方法において、

上記回数データ生成手段は、上記コンテンツデータの供給元に基づいて、当該コンテンツデータが経由した装置を示す経由装置データを生成し、

上記再送信手段は、上記コンテンツデータ及び上記残り回数データと共に、上記経由装置データを送信する。

115. 所定のプログラムを格納し、当該プログラムを情報送信装置に供給するプログラム格納媒体において、

上記プログラムは

所定のコンテンツデータと共に、当該コンテンツデータに対して予め規定した再送信可能な最大回数データを情報受信装置に送信する送信ステップを具える。



116. 所定のプログラムを格納し、当該プログラムを情報受信装置に供給するプログラム格納媒体において、

上記プログラムは、

情報送信装置から送信された所定のコンテンツデータと、当該コンテンツデータに対して予め規定した再送信可能な最大回数データとを受信する受信ステップと、

上記最大回数データに基づいて、上記コンテンツデータの再送信可能な残り回数データを生成する回数データ生成ステップと、

上記コンテンツデータと共に、上記残り回数データを送信する再送信ステップとを具える。

117. 請求の範囲第116項に記載のプログラム格納媒体において、

上記プログラムの上記回数データ生成手段は、上記コンテンツデータの供給元に基づいて、当該コンテンツデータが経由した装置を示す経由装置データを生成し、

上記再送信手段は、上記コンテンツデータ及び上記残り回数データと共に、上記経由装置データを送信する。

118. 情報送信装置から送信された所定のコンテンツデータを記録再生装置により着脱自在なデータ格納装置に記録再生する記録再生システムにおいて、

上記情報送信装置は、

上記コンテンツデータを所定のコンテンツ鍵で暗号化するコンテンツ暗号手段と、

上記コンテンツ鍵及び当該コンテンツ鍵で暗号化した上記コンテンツデータを送信する送信手段とを具え、

上記記録再生装置は、

上記情報送信装置から送信された上記コンテンツ鍵及び当該コンテンツ鍵で暗

号化されている上記コンテンツデータを受信する受信手段と、

受信した上記コンテンツ鍵及び当該コンテンツ鍵で暗号化されている上記コンテンツデータを上記データ格納装置に送出して記録させ、又は上記データ格納装置から上記コンテンツ鍵及び当該コンテンツ鍵で暗号化されている上記コンテンツデータを再生させて読み出す記録再生制御手段とを具え、

上記データ格納装置は、

所定の記録媒体と、

所定の保存鍵を保持する保存鍵保持手段と、

上記コンテンツ鍵を上記保存鍵で暗号化するコンテンツ鍵暗号手段と、

上記保存鍵で暗号化された上記コンテンツ鍵及び当該コンテンツ鍵で暗号化された上記コンテンツデータを上記記録媒体に記録し、又は当該記録媒体から上記保存鍵で暗号化された上記コンテンツ鍵及び当該コンテンツ鍵で暗号化された上記コンテンツデータを再生する記録再生手段と、

上記保存鍵で暗号化された上記コンテンツ鍵を当該保存鍵で復号化するコンテンツ鍵復号手段とを具える。

119. 請求の範囲第118項に記載の記録再生システムにおいて、

上記データ格納装置において、上記保存鍵保持手段は耐タンパ性を有する。

120. 請求の範囲第119項に記載の記録再生システムにおいて、

上記記録再生制御手段は、上記データ格納装置に対して上記記録媒体に記録された上記コンテンツ鍵で暗号化されている上記コンテンツデータの再生を制限する。

121. 請求の範囲第120項に記載の記録再生システムにおいて、

上記再生制限は、上記コンテンツデータの再生可能な回数でなる。

1 2 2. 請求の範囲第 1 2 0 項に記載の記録再生システムにおいて、  
上記再生制限は、上記コンテンツデータの再生可能な期間でなる。

1 2 3. 請求の範囲第 1 1 8 項に記載の記録再生システムにおいて、  
上記記録再生装置は、

上記データ格納装置から読み出した上記コンテンツ鍵で暗号化されている上記  
コンテンツデータを当該コンテンツ鍵を用いて復号化するコンテンツ復号手段を  
具える。

1 2 4. 請求の範囲第 1 1 8 項に記載の記録再生システムにおいて、

上記データ格納装置の上記記録媒体から上記コンテンツ鍵及び当該コンテンツ  
鍵で暗号化された上記コンテンツデータを再生させて読み出す再生制御手段を有  
し、上記データ格納装置が着脱自在に装填される再生装置を具える。

1 2 5. 請求の範囲第 1 2 4 項に記載の記録再生システムにおいて、  
上記再生装置は、

上記データ格納装置から読み出した上記コンテンツ鍵で暗号化されている上記  
コンテンツデータを当該コンテンツ鍵を用いて復号化するコンテンツ復号手段を  
具える。

1 2 6. 請求の範囲第 1 2 4 項に記載の記録再生システムにおいて、

上記再生制御手段は、上記データ格納装置に対して上記記録媒体に記録された  
上記コンテンツ鍵で暗号化されている上記コンテンツデータの再生を制限する。

1 2 7. 請求の範囲第 1 2 6 項に記載の記録再生システムにおいて、

上記再生制限は、上記コンテンツデータの再生可能な回数でなる。

1 2 8. 請求の範囲第 1 2 6 項に記載の記録再生システムにおいて、  
上記再生制限は、上記コンテンツデータの再生可能な期間でなる。

1 2 9. 請求の範囲第 1 1 8 項に記載の記録再生システムにおいて、  
上記データ格納装置の上記保存鍵保持手段は上記データ格納装置固有の上記保存鍵を保存する。

1 3 0. 所定の記録媒体を有するデータ格納装置が着脱自在に設けられた記録再生装置において、

所定のコンテンツ鍵で暗号化されているコンテンツデータと当該コンテンツ鍵とを上記データ格納装置に送出する送出手段と、

上記コンテンツ鍵を所定の保存鍵で暗号化して上記コンテンツ鍵で暗号化されている上記コンテンツデータを上記記録媒体に記録し、又は当該記録媒体から上記保存鍵で暗号化した上記コンテンツ鍵及び当該コンテンツ鍵で暗号化されている上記コンテンツデータを再生して上記保存鍵で暗号化した上記コンテンツ鍵を当該保存鍵で復号化する記録再生制御手段と、

上記データ格納装置から上記コンテンツ鍵及び当該コンテンツ鍵で暗号化されている上記コンテンツデータを読み出す読出手段とを具える。

1 3 1. 請求の範囲第 1 3 0 項に記載の記録再生装置において、

上記データ格納装置から読み出した上記コンテンツ鍵で暗号化されている上記コンテンツデータを当該コンテンツ鍵を用いて復号化するコンテンツ復号手段を具える。

1 3 2. 請求の範囲第 1 3 0 項に記載の記録再生装置において、

上記記録再生制御手段は、上記データ格納装置に対して上記記録媒体に記録された上記コンテンツ鍵で暗号化されている上記コンテンツデータの再生を制限す

る。

1 3 3. 請求の範囲第 1 3 2 項に記載の記録再生装置において、  
上記再生制限は、上記コンテンツデータの再生可能な回数でなる。

1 3 4. 請求の範囲第 1 3 2 項に記載の記録再生装置において、  
上記再生制限は、上記コンテンツデータの再生可能な期間でなる。

1 3 5. 請求の範囲第 1 3 0 項に記載の記録再生装置において、  
上記記録再生制御手段は、上記データ格納装置固有の上記保存鍵を用いて上記  
コンテンツ鍵を暗号化し、又は復号化する。

1 3 6. 所定の記録媒体を有するデータ格納装置が着脱自在に設けられた再生装  
置において、

上記記録媒体に予め記録された所定のコンテンツ鍵で暗号化されているコンテ  
ンツデータと、所定の保存鍵で暗号化されている上記コンテンツ鍵とを再生させ  
、上記保存鍵で暗号化されている上記コンテンツ鍵を当該保存鍵を用いて復号化  
する再生制御手段と、

上記データ格納装置から上記コンテンツ鍵及び当該コンテンツ鍵で暗号化され  
ている上記コンテンツデータを読み出す読出手段とを具える。

1 3 7. 請求の範囲第 1 3 6 項に記載の再生装置において、

上記データ格納装置から読み出した上記コンテンツ鍵で暗号化されている上記  
コンテンツデータを当該コンテンツ鍵を用いて復号化するコンテンツ復号手段を  
具える。

1 3 8. 請求の範囲第 1 3 6 項に記載の再生装置において、

上記再生制御手段は、上記データ格納装置に対して上記記録媒体に記録された上記コンテンツ鍵で暗号化されている上記コンテンツデータの再生を制限する。

139. 請求の範囲第138項に記載の再生装置において、  
上記再生制限は、上記コンテンツデータの再生可能な回数でなる。

140. 請求の範囲第138項に記載の再生装置において、  
上記再生制限は、上記コンテンツデータの再生可能な期間でなる。

141. 請求の範囲第136項に記載の再生装置において、  
上記再生制御手段は、上記データ格納装置固有の上記保存鍵を用いて上記コンテンツ鍵を復号化する。

142. 記録及び又は再生装置に着脱自在に設けられ、当該記録及び又は再生装置の制御のもとに、所定のデータを記録及び又は再生するデータ格納装置において、

所定の記録媒体と、

所定の保存鍵を保持する保存鍵保持手段と、

上記記録及び又は再生装置との間で、所定のコンテンツ鍵で暗号化した所定のコンテンツデータと、当該コンテンツ鍵とを送受信する通信手段と、

上記記録及び又は再生装置の制御のもとに、上記コンテンツ鍵を上記保存鍵で暗号化するコンテンツ鍵暗号手段と、

上記記録及び又は再生装置の制御のもとに、上記保存鍵で暗号化された上記コンテンツ鍵及び当該コンテンツ鍵で暗号化された上記コンテンツデータを上記記録媒体に記録し、又は当該記録媒体から上記保存鍵で暗号化された上記コンテンツ鍵及び当該コンテンツ鍵で暗号化された上記コンテンツデータを再生する記録再生手段と、

上記記録及び又は再生装置の制御のもとに、上記保存鍵で暗号化された上記コンテンツ鍵を当該保存鍵を用いて復号化するコンテンツ鍵復号手段とを具える。

1 4 3. 請求の範囲第 1 4 2 項に記載のデータ格納装置において、  
上記保存鍵保持手段は、耐タンパ性を有する。

1 4 4. 請求の範囲第 1 4 2 項に記載のデータ格納装置において、  
上記記録再生手段は、上記記録媒体に記録された上記コンテンツ鍵で暗号化されている上記コンテンツデータの再生を制限する。

1 4 5. 請求の範囲第 1 4 4 項に記載のデータ格納装置において、  
上記再生制限は、上記コンテンツデータの再生可能な回数でなる。

1 4 6. 請求の範囲第 1 4 4 項に記載のデータ格納装置において、  
上記再生制限は、上記コンテンツデータの再生可能な期間でなる。

1 4 7. 請求の範囲第 1 4 2 項に記載のデータ格納装置において、  
上記記録再生手段は、上記データ格納装置固有の上記保存鍵を用いて上記コンテンツ鍵を暗号化し、又は復号化する。

1 4 8. 情報送信装置から送信された所定のコンテンツデータを記録再生装置により着脱自在なデータ格納装置に記録再生する記録再生方法において、

上記情報送信装置により上記コンテンツデータを所定のコンテンツ鍵で暗号化するコンテンツ暗号ステップと、

上記情報送信装置により上記コンテンツ鍵及び当該コンテンツ鍵で暗号化した上記コンテンツデータを送信する送信ステップと、

上記記録再生装置により上記情報送信装置から送信された上記コンテンツ鍵及

び当該コンテンツ鍵で暗号化された上記コンテンツデータを受信する受信ステップと、

上記記録再生装置により上記コンテンツ鍵及び当該コンテンツ鍵で暗号化されている上記コンテンツデータを上記データ格納装置に送出し、上記コンテンツ鍵を上記データ格納装置に予め保持している保存鍵で暗号化して当該コンテンツ鍵で暗号化されている上記コンテンツデータと共に上記データ格納装置の記録媒体に記録し、又は当該記録媒体から上記保存鍵で暗号化した上記コンテンツ鍵及び当該コンテンツ鍵で暗号化されている上記コンテンツデータを再生し、上記データ格納装置から上記保存鍵で暗号化した上記コンテンツ鍵を上記保存鍵で復号化して上記コンテンツ鍵で暗号化されている上記コンテンツデータと共に読み出す記録再生制御ステップとを具える。

149. 請求の範囲第148項に記載の記録再生方法において、

上記記録再生制御ステップは、上記データ格納装置内の耐タンパ性を有する所定の保存鍵保持手段に保持している上記保存鍵を上記コンテンツ鍵の記録再生に用いる。

150. 請求の範囲第148項に記載の記録再生方法において、

上記記録再生制御ステップは、上記データ格納装置の上記記録媒体に記録した上記コンテンツ鍵で暗号化されている上記コンテンツデータの再生を制限する。

151. 請求の範囲第150項に記載の記録再生方法において、

上記記録再生制御ステップは、上記データ格納装置の上記記録媒体に記録した上記コンテンツ鍵で暗号化されている上記コンテンツデータの再生の制限として、再生可能な回数を制限する。

152. 請求の範囲第150項に記載の記録再生方法において、



上記記録再生制御ステップは、上記データ格納装置の上記記録媒体に記録した上記コンテンツ鍵で暗号化されている上記コンテンツデータの再生の制限として、再生可能な期間を制限する。

153. 請求の範囲第148項に記載の記録再生方法において、

上記記録再生装置により上記データ格納装置から読み出した上記コンテンツ鍵で暗号化されている上記コンテンツデータを当該コンテンツ鍵を用いて復号化するコンテンツ復号ステップを具える。

154. 請求の範囲第148項に記載の記録再生方法において、

上記記録再生制御ステップは、上記データ格納装置固有の上記保存鍵を用いて上記コンテンツ鍵を暗号化し、又は復号化する。

155. 請求の範囲第148項に記載の記録再生方法において、

上記データ格納装置が着脱自在に装填される再生装置により上記データ格納装置の上記記録媒体から上記コンテンツ鍵及び当該コンテンツ鍵で暗号化されている上記コンテンツデータを再生して読み出す再生制御ステップを具える。

156. 請求の範囲第155項に記載の記録再生方法において、

上記再生制御ステップは、上記データ格納装置の上記記録媒体に記録した上記コンテンツ鍵で暗号化されている上記コンテンツデータの再生を制限する。

157. 請求の範囲第156項に記載の記録再生方法において、

上記再生制御ステップは、上記データ格納装置の上記記録媒体に記録した上記コンテンツ鍵で暗号化されている上記コンテンツデータの再生の制限として、再生可能な回数を制限する。

158. 請求の範囲第156項に記載の記録再生方法において、

上記再生制御ステップは、上記データ格納装置の上記記録媒体に記録した上記コンテンツ鍵で暗号化されている上記コンテンツデータの再生の制限として、再生可能な期間を制限する。

159. 請求の範囲第156項に記載の記録再生方法において、

上記再生装置により上記データ格納装置から読み出した上記コンテンツ鍵で暗号化されている上記コンテンツデータを当該コンテンツ鍵を用いて復号化するコンテンツ復号手段ステップを具える。

160. 請求の範囲第155項に記載の記録再生方法において、

上記再生制御ステップは、上記データ格納装置固有の上記保存鍵を用いて上記コンテンツ鍵を復号化する。

161. 記録再生装置に着脱自在に設けられたデータ格納装置の記録媒体に所定のコンテンツデータを記録再生する記録再生方法において、

上記記録再生装置から所定のコンテンツ鍵で暗号化されているコンテンツデータと、当該コンテンツ鍵とを上記データ格納装置に送出する送出ステップと、

上記記録再生装置の制御のもとに、上記コンテンツ鍵を所定の保存鍵で暗号化して上記コンテンツ鍵で暗号化されている上記コンテンツデータと共に上記記録媒体に記録し、又は当該記録媒体から上記保存鍵で暗号化した上記コンテンツ鍵及び当該コンテンツ鍵で暗号化されている上記コンテンツデータを再生し、上記保存鍵で暗号化した上記コンテンツ鍵を当該保存鍵を用いて復号化する記録再生ステップと、

上記記録再生装置に上記データ格納装置から復号化した上記コンテンツ鍵及び上記コンテンツ鍵で暗号化されている上記コンテンツデータを読み出す読出ステップとを具える。

162. 請求の範囲第161項に記載の記録再生方法において、

上記記録再生装置により、上記データ格納装置から読み出した上記コンテンツ鍵で暗号化されている上記コンテンツデータを当該コンテンツ鍵を用いて復号化するコンテンツ復号ステップを具える。

163. 請求の範囲第161項に記載の記録再生方法において、

上記記録再生ステップは、上記記録再生装置の制御のもとに、上記データ格納装置の上記記録媒体に記録した上記コンテンツ鍵で暗号化されている上記コンテンツデータの再生を制限する。

164. 請求の範囲第163項に記載の記録再生方法において、

上記記録再生ステップは、上記記録再生装置の制御のもとに、上記データ格納装置の上記記録媒体に記録した上記コンテンツ鍵で暗号化されている上記コンテンツデータの再生の制限として、再生可能な回数を制限する。

165. 請求の範囲第163項に記載の記録再生方法において、

上記記録再生ステップは、上記記録再生装置の制御のもとに、上記データ格納装置の上記記録媒体に記録した上記コンテンツ鍵で暗号化されている上記コンテンツデータの再生の制限として、再生可能な期間を制限する。

166. 請求の範囲第161項に記載の記録再生方法において、

上記記録再生ステップは、上記データ格納装置固有の上記保存鍵を用いて上記コンテンツ鍵を暗号化し、又は復号化する。

167. 再生装置に着脱自在に設けられたデータ格納装置の記録媒体から予め記録された所定のコンテンツデータを再生する再生方法において、

上記再生装置の制御のもとに、上記データ格納装置の上記記録媒体から予め記

録された所定のコンテンツ鍵で暗号化されているコンテンツデータと、所定の保存鍵で暗号化されている上記コンテンツ鍵とを再生する再生ステップと、

上記再生装置の制御のもとに、上記保存鍵で暗号化されている上記コンテンツ鍵を当該保存鍵を用いて復号化する復号ステップと、

上記再生装置に上記コンテンツ鍵及び上記コンテンツ鍵で暗号化されている上記コンテンツデータを上記データ格納装置から読み出す読出ステップとを具える。

168. 請求の範囲第167項に記載の再生方法において、

上記再生装置により上記データ格納装置から読み出した上記コンテンツ鍵で暗号化されている上記コンテンツデータを当該コンテンツ鍵を用いて復号化するコンテンツ復号ステップを具える。

169. 請求の範囲第167項に記載の再生方法において、

上記再生ステップは、上記再生装置の制御のもとに、上記データ格納装置の上記記録媒体に記録した上記コンテンツ鍵で暗号化されている上記コンテンツデータの再生を制限する。

170. 請求の範囲第169項に記載の再生方法において、

上記再生ステップは、上記再生装置の制御のもとに、上記データ格納装置の上記記録媒体に記録した上記コンテンツ鍵で暗号化されている上記コンテンツデータの再生の制限として、再生可能な回数を制限する。

171. 請求の範囲第169項に記載の再生方法において、

上記再生ステップは、上記再生装置の制御のもとに、上記データ格納装置の上記記録媒体に記録した上記コンテンツ鍵で暗号化されている上記コンテンツデータの再生の制限として、再生可能な期間を制限する。

172. 請求の範囲第167項に記載の再生方法において、

上記復号ステップは、上記データ格納装置固有の上記保存鍵を用いて上記コンテンツ鍵を復号化する。

173. 所定のプログラムを格納し、当該プログラムを記録再生装置に供給するプログラム格納媒体において、

上記プログラムは、

上記記録再生装置に着脱自在に設けられたデータ格納装置に所定のコンテンツ鍵で暗号化されているコンテンツデータと、当該コンテンツ鍵とを送出する送出ステップと、

上記コンテンツ鍵を所定の保存鍵で暗号化して上記コンテンツ鍵で暗号化されている上記コンテンツデータと共に上記データ格納装置の有する所定の記録媒体に記録し、又は当該記録媒体から上記保存鍵で暗号化した上記コンテンツ鍵及び当該コンテンツ鍵で暗号化されている上記コンテンツデータを再生し、上記保存鍵で暗号化した上記コンテンツ鍵を当該保存鍵を用いて復号化するように上記データ格納装置を制御する記録再生制御ステップと、

上記データ格納装置から復号化した上記コンテンツ鍵及び上記コンテンツ鍵で暗号化されている上記コンテンツデータを読み出す読出ステップとを具える。

174. 請求の範囲第173項に記載のプログラム格納媒体において、

上記プログラムは、

上記データ格納装置から読み出した上記コンテンツ鍵で暗号化されている上記コンテンツデータを当該コンテンツ鍵を用いて復号化するコンテンツ復号ステップを具える。

175. 請求の範囲第173項に記載のプログラム格納媒体において、

上記プログラムの上記記録再生制御ステップは、上記記録再生装置の制御のも

とに、上記データ格納装置の上記記録媒体に記録した上記コンテンツ鍵で暗号化されている上記コンテンツデータの再生を制限する。

176. 請求の範囲第175項に記載のプログラム格納媒体において、

上記プログラムの上記記録再生制御ステップは、上記記録再生装置の制御のもとに、上記データ格納装置の上記記録媒体に記録した上記コンテンツ鍵で暗号化されている上記コンテンツデータの再生の制限として、再生可能な回数を制限する。

177. 請求の範囲第175項に記載のプログラム格納媒体において、

上記プログラムの上記記録再生制御ステップは、上記記録再生装置の制御のもとに、上記データ格納装置の上記記録媒体に記録した上記コンテンツ鍵で暗号化されている上記コンテンツデータの再生の制限として、再生可能な期間を制限する。

178. 請求の範囲第173項に記載のプログラム格納媒体において、

上記プログラムの上記記録再生制御ステップは、上記データ格納装置固有の上記保存鍵を用いて上記コンテンツ鍵を暗号化し、又は復号化する。

179. 所定のプログラムを格納し、当該プログラムを再生装置に供給するプログラム格納媒体において、

上記プログラムは、

上記再生装置に着脱自在に設けられたデータ格納装置の記録媒体から予め記録された所定のコンテンツ鍵で暗号化されているコンテンツデータと、所定の保存鍵で暗号化されている上記コンテンツ鍵とを再生するように上記データ格納装置を制御する再生制御ステップと、

上記保存鍵で暗号化されている上記コンテンツ鍵を当該保存鍵を用いて復号化

するように上記データ格納装置を制御する復号制御ステップと、

上記データ格納装置から上記コンテンツ鍵及び上記コンテンツ鍵で暗号化されている上記コンテンツデータを読み出す読出ステップとを具える。

180. 請求の範囲第179項に記載のプログラム格納媒体において、

上記プログラムは、

上記再生装置により上記データ格納装置から読み出した上記コンテンツ鍵で暗号化されている上記コンテンツデータを当該コンテンツ鍵を用いて復号化するコンテンツ復号ステップを具える。

181. 請求の範囲第179項に記載のプログラム格納媒体において、

上記プログラムの上記再生制御ステップは、上記データ格納装置の上記記録媒体に記録した上記コンテンツ鍵で暗号化されている上記コンテンツデータの再生を制限する。

182. 請求の範囲第181項に記載のプログラム格納媒体において、

上記プログラムの上記再生制御ステップは、上記データ格納装置の上記記録媒体に記録した上記コンテンツ鍵で暗号化されている上記コンテンツデータの再生の制限として、再生可能な回数を制限する。

183. 請求の範囲第181項に記載のプログラム格納媒体において、

上記プログラムの上記再生制御ステップは、上記データ格納装置の上記記録媒体に記録した上記コンテンツ鍵で暗号化されている上記コンテンツデータの再生の制限として、再生可能な期間を制限する。

184. 請求の範囲第179項に記載のプログラム格納媒体において、

上記プログラムの上記復号制御ステップは、上記データ格納装置固有の上記保

存鍵を用いて上記コンテンツ鍵を復号化する。

185. 所定のプログラムを格納し、当該プログラムをデータ格納装置に供給するプログラム格納媒体において、

上記プログラムは、

上記データ格納装置が着脱自在に設けられた記録再生装置から送信された、所定のコンテンツ鍵で暗号化されているコンテンツデータと、当該コンテンツ鍵とを受信する受信ステップと、

上記記録再生装置の制御のもとに、上記コンテンツ鍵を所定の保存鍵で暗号化して上記コンテンツ鍵で暗号化されている上記コンテンツデータと共に上記データ格納装置の有する所定の記録媒体に記録し、又は当該記録媒体から上記保存鍵で暗号化した上記コンテンツ鍵及び当該コンテンツ鍵で暗号化されている上記コンテンツデータを再生し、上記保存鍵で暗号化した上記コンテンツ鍵を当該保存鍵を用いて復号化する記録再生ステップと、

上記コンテンツ鍵及び上記コンテンツ鍵で暗号化されている上記コンテンツデータを上記記録再生装置に送信する送信ステップとを具える。

186. 請求の範囲第185項に記載のプログラム格納媒体において、

上記プログラムの上記記録再生ステップは、上記記録再生装置の制御のもとに、上記データ格納装置の上記記録媒体に記録した上記コンテンツ鍵で暗号化されている上記コンテンツデータの再生を制限する。

187. 請求の範囲第186項に記載のプログラム格納媒体において、

上記プログラムの上記記録再生ステップは、上記記録再生装置の制御のもとに、上記データ格納装置の上記記録媒体に記録した上記コンテンツ鍵で暗号化されている上記コンテンツデータの再生の制限として、再生可能な回数を制限する。



188. 請求の範囲第186項に記載のプログラム格納媒体において、

上記プログラムの上記記録再生ステップは、上記記録再生装置の制御のもとに、上記データ格納装置の上記記録媒体に記録した上記コンテンツ鍵で暗号化されている上記コンテンツデータの再生の制限として、再生可能な期間を制限する。

189. 請求の範囲第185項に記載のプログラム格納媒体において、

上記プログラムの上記記録再生ステップは、上記データ格納装置固有の上記保存鍵を用いて上記コンテンツ鍵を暗号化し、又は復号化する。

190. 所定のプログラムを格納し、当該プログラムをデータ格納装置に供給するプログラム格納媒体において、

上記プログラムは、

上記データ格納装置が着脱自在に設けられた再生装置の制御のもとに、上記データ格納装置の記録媒体から予め記録された所定のコンテンツ鍵で暗号化されているコンテンツデータと、所定の保存鍵で暗号化されている上記コンテンツ鍵とを再生する再生ステップと、

上記再生装置の制御のもとに、上記保存鍵で暗号化されている上記コンテンツ鍵を当該保存鍵を用いて復号化する復号ステップと、

上記コンテンツ鍵及び上記コンテンツ鍵で暗号化されている上記コンテンツデータを上記再生装置に送信する送信ステップとを具える。

191. 請求の範囲第190項に記載のプログラム格納媒体において、

上記プログラムの上記再生ステップは、上記再生装置の制御のもとに、上記記録媒体に記録した上記コンテンツ鍵で暗号化されている上記コンテンツデータの再生を制限する。

192. 請求の範囲第191項に記載のプログラム格納媒体において、

上記プログラムの上記再生ステップは、上記再生装置の制御のもとに、上記記録媒体に記録した上記コンテンツ鍵で暗号化されている上記コンテンツデータの再生の制限として、再生可能な回数を制限する。

193. 請求の範囲第191項に記載のプログラム格納媒体において、

上記プログラムの上記再生ステップは、上記再生装置の制御のもとに、上記記録媒体に記録した上記コンテンツ鍵で暗号化されている上記コンテンツデータの再生の制限として、再生可能な期間を制限する。

194. 請求の範囲第190項に記載のプログラム格納媒体において、

上記プログラムの上記復号ステップは、上記データ格納装置固有の上記保存鍵を用いて上記コンテンツ鍵を復号化する。

195. データ管理システムにおいて、

所定の記録媒体を有する着脱自在なデータ格納装置と、

上記データ格納装置の上記記録媒体に所定のコンテンツデータを記録する記録装置と、

各種機器に接続され、上記データ格納装置の記録媒体に記録された上記コンテンツデータを取り込んで当該コンテンツデータの各種機器への移動を上記データ格納装置に代えて管理する管理装置とを具える。

196. 請求の範囲第195項に記載のデータ管理システムにおいて、

上記記録装置は、

着脱自在な上記データ格納装置に、所定のコンテンツ鍵で暗号化されている上記コンテンツデータと、当該コンテンツ鍵と、当該コンテンツ鍵の使用条件を規定した取扱方針とを送信する送信手段と、

上記取扱方針に基づいて上記コンテンツデータの利用権を規定し、当該コンテ

ンツデータの保持者を識別するための識別情報を格納した使用許諾条件情報を作成させて、当該使用許諾条件情報と、上記コンテンツ鍵で暗号化されている上記コンテンツデータ及び当該コンテンツ鍵並びに上記取扱方針とを上記記録媒体に記録するように上記データ格納装置を制御する記録制御手段とを具え、

上記管理装置は、

上記データ格納装置の上記記録媒体から上記コンテンツ鍵で暗号化されている上記コンテンツデータと、当該コンテンツ鍵と、上記使用許諾条件情報とを再生して取り込む取込手段と、

上記使用許諾条件情報を上記識別情報を変更して更新し、当該更新した上記使用許諾条件情報と共に、上記コンテンツ鍵で暗号化されている上記コンテンツデータと、当該コンテンツ鍵とを上記各種機器へ移動させる移動管理手段とを具える。

197. 請求の範囲第196項に記載のデータ管理システムにおいて、

上記管理装置の上記取込手段は、上記各種機器から上記使用許諾条件情報に基づいて返還される当該使用許諾条件情報と、上記コンテンツ鍵で暗号化されている上記コンテンツデータと、当該コンテンツ鍵とを取り込む。

198. 請求の範囲第196項に記載のデータ管理システムにおいて、

上記記録装置の上記記録制御手段は、上記取扱方針に基づいて上記コンテンツデータの利用権を規定し、上記データ格納装置固有の上記識別情報を格納した上記使用許諾条件情報を作成させ、

上記管理装置の上記管理移動手段は、上記使用許諾条件情報内の上記データ格納装置固有の上記識別情報を上記管理装置固有の上記識別情報に変更して上記使用許諾条件情報を更新する。

199. 請求の範囲第198項に記載のデータ管理システムにおいて、

上記記録装置の上記送信手段は、上記データ格納装置に、上記コンテンツ鍵で暗号化されている上記コンテンツデータと、当該コンテンツ鍵と、上記取扱方針に加えて上記コンテンツデータの価格情報を送信し、

上記記録制御手段は、上記データ格納装置に上記取扱方針及び上記価格情報に基づいて上記コンテンツデータの購入に対する課金情報を生成させて所定のメモリに保持させ、

上記管理装置の上記取込手段は、上記コンテンツ鍵で暗号化されている上記コンテンツデータ、当該コンテンツ鍵及び上記使用許諾条件情報と共に、上記課金情報を取り込む。

200. 請求の範囲第199項に記載のデータ管理システムにおいて、

上記管理装置の上記取込手段は、上記管理装置と上記データ格納装置との間で共有化した一時鍵で暗号化されている上記コンテンツ鍵と、当該一時鍵で暗号化されている上記課金情報とを取り込む。

201. 請求の範囲第200項に記載のデータ管理システムにおいて、

上記管理装置の上記取込手段は、上記データ格納装置から上記一時鍵で暗号化された後、署名データが付加された上記課金情報を取り込む。

202. 各種機器と着脱自在な所定のデータ格納装置とが接続される管理装置において、

上記データ格納装置の記録媒体に記録された所定のコンテンツデータを再生して取り込む取込手段と、

上記コンテンツデータの各種機器への移動を上記データ格納装置に代えて管理する移動管理手段とを具える。

203. 請求の範囲第202項に記載の管理装置において、

上記取込手段は、上記データ格納装置の上記記録媒体から所定のコンテンツ鍵で暗号化されている上記コンテンツデータと、当該コンテンツ鍵と、当該コンテンツ鍵の使用条件を規定した取扱方針に基づいて生成された上記コンテンツデータの利用権を規定し、当該コンテンツデータの保持者を識別するための識別情報を格納した使用許諾条件情報とを取り込み、

上記移動管理手段は、上記使用許諾条件情報を上記識別情報を変更して更新し、当該更新した上記使用許諾条件情報と共に、上記コンテンツ鍵で暗号化されている上記コンテンツデータと、当該コンテンツ鍵とを上記各種機器へ移動させる。

204. 請求の範囲第202項に記載の管理装置において、

上記取込手段は、上記各種機器から上記使用許諾条件情報に基づいて返還される当該使用許諾条件情報と、上記コンテンツ鍵で暗号化されている上記コンテンツデータと、当該コンテンツ鍵とを取り込む。

205. 請求の範囲第203項に記載の管理装置において、

上記取込手段は、上記データ格納装置固有の上記識別情報が格納された上記使用許諾条件情報を取り込み、

上記管理移動手段は、上記使用許諾条件情報内の上記データ格納装置固有の上記識別情報を上記管理装置固有の上記識別情報に変更して上記使用許諾条件情報を更新する。

206. 請求の範囲第205項に記載の管理装置において、

上記取込手段は、上記データ格納装置から上記取扱方針及び上記コンテンツデータの価格情報に基づいて生成された上記コンテンツデータの購入に対する課金情報を取り込む。

207. 請求の範囲第206項に記載の管理装置において、

上記管理装置と上記データ格納装置との間で共有化した一時鍵で暗号化されている所定のデータを当該一時鍵で復号化する復号手段を具え、

上記取込手段は、上記データ格納装置から上記一時鍵で暗号化されている上記コンテンツ鍵と、当該一時鍵で暗号化されている上記課金情報とを取り込み、

上記復号手段は、上記一時鍵で暗号化されている上記コンテンツ鍵と、上記課金情報とをそれぞれ上記一時鍵で復号化する。

208. 請求の範囲第207項に記載の管理装置において、

所定のデータに付加された署名データを検証して上記データの改竄の有無を検出する検出手段を具え、

上記取込手段は、上記データ格納装置から上記一時鍵で暗号化された後、署名データが付加された上記課金情報を取り込み、

上記検出手段は、上記一時鍵で暗号化された上記課金情報に付加されている上記署名を検証する。

209. 所定の記録媒体を有する着脱自在なデータ格納装置において、

所定の記録装置に接続された際に当該記録装置から送信された所定のコンテンツ鍵で暗号化されているコンテンツデータと、当該コンテンツ鍵と、当該コンテンツ鍵の使用条件を規定した取扱方針と受信する受信手段と、

上記記録装置の制御のもとに、上記取扱方針に基づいて上記コンテンツデータの利用権を規定し、当該コンテンツデータの保持者を識別するための識別情報を格納した使用許諾条件情報を作成する情報作成手段と、

上記記録装置の制御のもとに、上記使用許諾条件情報と、上記コンテンツ鍵で暗号化されている上記コンテンツデータ及び当該コンテンツ鍵並びに上記取扱方針とを上記記録媒体に記録する記録手段と、

各種機器への上記コンテンツデータの移動を管理する管理装置に接続された際

に、当該管理装置の制御のもとに、上記記録媒体から上記コンテンツ鍵で暗号化されている上記コンテンツデータと、当該コンテンツ鍵と、上記使用許諾条件情報とを再生する再生手段と、

上記管理装置の制御のもとに、上記コンテンツ鍵で暗号化されている上記コンテンツデータ及び当該コンテンツ鍵と共に、上記コンテンツデータを管理するための上記使用許諾条件情報を上記管理装置に送信して上記コンテンツデータの管理を移行する送信手段とを具える。

210. 請求の範囲第209項に記載のデータ格納装置において、

上記情報作成手段は、上記取扱方針に基づいて、上記コンテンツデータの利用権を規定し、当該コンテンツデータの保持者を識別するための変更可能な識別情報を格納した使用許諾条件情報を作成する。

211. 請求の範囲第210項に記載のデータ格納装置において、

上記情報作成手段は、上記データ格納装置固有の上記識別情報が格納された上記使用許諾条件情報を作成する。

212. 請求の範囲第211項に記載のデータ格納装置において、

上記受信手段は、上記記録装置から上記コンテンツ鍵で暗号化されているコンテンツデータと、当該コンテンツ鍵と、上記取扱方針と共に送信された上記コンテンツデータの価格情報を受信し、

上記情報作成手段は、上記取扱方針及び上記価格情報に基づいて上記コンテンツデータの購入に対する課金情報を作成し所定のメモリに記録する。

213. 請求の範囲第212項に記載のデータ格納装置において、

上記情報作成手段は、耐タンパ性を有する上記メモリに上記課金情報を記録する。

214. 請求の範囲第213項に記載のデータ格納装置において、

上記管理装置との間で共有化した一時鍵で上記コンテンツ鍵を暗号化すると共に、当該一時鍵で上記課金情報を暗号化する暗号化手段を具え、

上記送信手段は、上記コンテンツ鍵で暗号化されている上記コンテンツデータ及び上記使用許諾条件情報と共に、上記一時鍵で暗号化した上記コンテンツ鍵と、上記一時鍵で暗号化した上記課金情報とを上記管理装置に送信する。

215. 請求の範囲第214項に記載のデータ格納装置において、

上記一時鍵で暗号化された上記課金情報に、改竄の有無を検証するための署名データを付加する付加手段を具え、

上記送信手段は、上記コンテンツ鍵で暗号化されている上記コンテンツデータ、上記使用許諾条件情報及び上記一時鍵で暗号化した上記コンテンツ鍵と共に上記一時鍵で暗号化して署名データが付加された上記課金情報を上記管理装置に送信する。

216. データ管理方法において、

所定の記録装置により、着脱自在なデータ格納装置に所定のコンテンツデータを送信する送信ステップと、

上記記録装置の制御のもとに、上記データ格納装置の記録媒体に上記コンテンツデータを記録する記録ステップと、

各種機器に接続される管理装置により、上記データ格納装置の記録媒体から上記コンテンツデータを再生して取り込む取込ステップと、

管理装置により、上記コンテンツデータの各種機器への移動を上記データ格納装置に代えて管理する移動管理ステップとを具える。

217. 請求の範囲第216項に記載のデータ管理方法において、

上記送信ステップは、上記データ格納装置に所定のコンテンツ鍵で暗号化され



ている上記コンテンツデータと、当該コンテンツ鍵と、当該コンテンツ鍵の使用条件を規定した取扱方針とを送信し、

上記記録ステップは、上記コンテンツ鍵で暗号化されている上記コンテンツデータと、当該コンテンツ鍵と、当該コンテンツ鍵の使用条件を規定した取扱方針とを上記記録媒体に記録すると共に、上記データ格納装置により上記取扱方針に基づいて、上記コンテンツデータの利用権を規定し、当該コンテンツデータの保持者を識別するための識別情報を格納した使用許諾条件情報を作成させて上記記録媒体に記録し、

上記取込ステップは、上記データ格納装置の上記記録媒体から上記コンテンツ鍵で暗号化されている上記コンテンツデータと、当該コンテンツ鍵と、上記使用許諾条件情報とを再生して取り込み、

上記移動管理ステップは、上記使用許諾条件情報を上記識別情報を変更して更新し、当該更新した上記使用許諾条件情報と共に、上記コンテンツ鍵で暗号化されている上記コンテンツデータと、当該コンテンツ鍵とを上記各種機器へ移動させる。

218. 請求の範囲第217項に記載のデータ管理方法において、

上記管理装置により、上記各種機器から上記使用許諾条件情報に基づいて返還される当該使用許諾条件情報と、上記コンテンツ鍵で暗号化されている上記コンテンツデータと、当該コンテンツ鍵とを取り込む取込みステップを具える。

219. 請求の範囲第217項に記載のデータ管理方法において、

上記記録ステップは、上記取扱方針に基づいて上記コンテンツデータの利用権を規定し、上記データ格納装置固有の上記識別情報を格納した上記使用許諾条件情報を作成し、

上記移動管理ステップは、上記使用許諾条件情報内の上記データ格納装置固有の上記識別情報を上記管理装置固有の上記識別情報に変更して上記使用許諾条件

情報を更新する。

220. 請求の範囲第219項に記載のデータ管理方法において、

上記送信ステップは、上記記録装置から上記データ格納装置に上記コンテンツ鍵で暗号化されている上記コンテンツデータと、当該コンテンツ鍵と、上記取扱方針とに加えて上記コンテンツデータの価格情報を送信し、

上記記録ステップは、上記データ格納装置により上記取扱方針及び上記価格情報に基づいて上記コンテンツデータの購入に対する課金情報を生成させて所定のメモリに保持し、

上記取込ステップは、上記コンテンツ鍵で暗号化されている上記コンテンツデータ、当該コンテンツ鍵及び上記使用許諾条件情報と共に上記課金情報を取り込む。

221. 請求の範囲第220項に記載のデータ管理方法において、

上記取込ステップは、上記データ格納装置の上記記録媒体から再生された後、上記管理装置と上記データ格納装置との間で共有化した一時鍵で暗号化されている上記コンテンツ鍵と、当該一時鍵で暗号化されている上記課金情報とを取り込む。

222. 請求の範囲第221項に記載のデータ管理方法において、

上記取込ステップは、上記データ格納装置から上記一時鍵で暗号化された後、署名データが付加された上記課金情報を取り込む。

223. 各種機器と着脱自在な所定のデータ格納装置とが接続される管理装置のデータ管理方法において、

上記データ格納装置の記録媒体に記録された所定のコンテンツデータを再生して取り込む取込ステップと、

上記コンテンツデータの各種機器への移動を上記データ格納装置に代えて管理する移動管理ステップとをを具える。

224. 請求の範囲第223項に記載のデータ管理方法において、

上記取込ステップは、上記データ格納装置の上記記録媒体から所定のコンテンツ鍵で暗号化されている上記コンテンツデータと、当該コンテンツ鍵と、当該コンテンツ鍵の使用条件を規定した取扱方針に基づいて生成された上記コンテンツデータの利用権を規定し、当該コンテンツデータの保持者を識別するための識別情報を格納した使用許諾条件情報とを取り込み、

上記移動管理ステップは、上記使用許諾条件情報を上記識別情報を変更して更新し、当該更新した上記使用許諾条件情報と共に、上記コンテンツ鍵で暗号化されている上記コンテンツデータと、当該コンテンツ鍵とを上記各種機器へ移動させる。

225. 請求の範囲第223項に記載のデータ管理方法において、

上記取込ステップは、上記各種機器から上記使用許諾条件情報に基づいて返還される当該使用許諾条件情報と、上記コンテンツ鍵で暗号化されている上記コンテンツデータと、当該コンテンツ鍵とを取り込む。

226. 請求の範囲第224項に記載のデータ管理方法において、

上記取込ステップは、上記データ格納装置固有の上記識別情報が格納された上記使用許諾条件情報を取り込み、

上記管理移動ステップは、上記使用許諾条件情報内の上記データ格納装置固有の上記識別情報を上記管理装置固有の上記識別情報に変更して上記使用許諾条件情報を更新する。

227. 請求の範囲第226項に記載のデータ管理方法において、

上記取込ステップは、上記データ格納装置から上記取扱方針及び上記コンテンツデータの価格情報に基づいて生成された上記コンテンツデータの購入に対する課金情報を取り込む。

228. 請求の範囲第227項に記載のデータ管理方法において、

上記管理装置と上記データ格納装置との間で共有化した一時鍵で暗号化されている所定のデータを当該一時鍵で復号化する復号ステップを具え、

上記取込ステップは、上記データ格納装置から上記一時鍵で暗号化されている上記コンテンツ鍵と、当該一時鍵で暗号化されている上記課金情報とを取り込み、

上記復号ステップは、上記一時鍵で暗号化されている上記コンテンツ鍵と、上記課金情報とをそれぞれ上記一時鍵で復号化する。

229. 請求の範囲第228項に記載のデータ管理方法において、

所定のデータに付加された署名データを検証して上記データの改竄の有無を検出する検出ステップを具え、

上記取込ステップは、上記データ格納装置から上記一時鍵で暗号化された後、署名データが付加された上記課金情報を取り込み、

上記検出ステップは、上記一時鍵で暗号化された上記課金情報に付加されている上記署名を検証する。

230. 所定の記録媒体を有する着脱自在なデータ格納装置に対するデータ管理移動方法において、

所定の記録装置から上記データ格納装置に送信された所定のコンテンツ鍵で暗号化されているコンテンツデータと、当該コンテンツ鍵と、当該コンテンツ鍵の使用条件を規定した取扱方針と受信する受信ステップと、

上記記録装置の制御のもとに、上記取扱方針に基づいて上記コンテンツデータ

の利用権を規定し、当該コンテンツデータの保持者を識別するための識別情報を格納した使用許諾条件情報を作成する情報作成ステップと、

上記記録装置の制御のもとに、上記使用許諾条件情報と、上記コンテンツ鍵で暗号化されている上記コンテンツデータ及び当該コンテンツ鍵並びに上記取扱方針とを上記記録媒体に記録する記録ステップと、

各種機器への上記コンテンツデータの移動を管理する管理装置に上記データ格納装置が接続された際に、当該管理装置の制御のもとに、上記記録媒体から上記コンテンツ鍵で暗号化されている上記コンテンツデータと、当該コンテンツ鍵と、上記使用許諾条件情報とを再生する再生ステップと、

上記管理装置の制御のもとに、上記データ格納装置から上記コンテンツ鍵で暗号化されている上記コンテンツデータ及び当該コンテンツ鍵と共に、上記コンテンツデータを管理するための上記使用許諾条件情報を上記管理装置に送信して上記コンテンツデータの管理を移行する送信ステップとを具える。

231. 請求の範囲第230項に記載のデータ管理移動方法において、

上記情報作成ステップは、上記取扱方針に基づいて、上記コンテンツデータの利用権を規定し、当該コンテンツデータの保持者を識別するための変更可能な識別情報を格納した使用許諾条件情報を作成する。

232. 請求の範囲第231項に記載のデータ管理移動方法において、

上記情報作成ステップは、上記データ格納装置固有の上記識別情報が格納された上記使用許諾条件情報を作成する。

233. 請求の範囲第232項に記載のデータ管理移動方法において、

上記受信ステップは、上記記録装置から上記コンテンツ鍵で暗号化されているコンテンツデータと、当該コンテンツ鍵と、上記取扱方針と共に送信された上記コンテンツデータの価格情報を受信し、

上記情報作成ステップは、上記取扱方針及び上記価格情報に基づいて上記コンテンツデータの購入に対する課金情報を作成し所定のメモリに記録する。

234. 請求の範囲第233項に記載のデータ管理移動方法において、

上記情報作成ステップは、耐タンパ性を有する上記メモリに上記課金情報を記録する。

235. 請求の範囲第234項に記載のデータ管理移動方法において、

上記管理装置との間で共有化した一時鍵で上記コンテンツ鍵を暗号化すると共に、当該一時鍵で上記課金情報を暗号化する暗号化ステップを具え、

上記送信ステップは、上記コンテンツ鍵で暗号化されている上記コンテンツデータ及び上記使用許諾条件情報と共に、上記一時鍵で暗号化した上記コンテンツ鍵と、上記一時鍵で暗号化した上記課金情報とを上記管理装置に送信する。

236. 請求の範囲第235項に記載のデータ管理移動方法において、

上記一時鍵で暗号化された上記課金情報に、改竄の有無を検証するための署名データを付加する付加ステップを具え、

上記送信ステップは、上記コンテンツ鍵で暗号化されている上記コンテンツデータ、上記使用許諾条件情報及び上記一時鍵で暗号化した上記コンテンツ鍵と共に上記一時鍵で暗号化して署名データが付加された上記課金情報を上記管理装置に送信する。

237. 所定のプログラムを格納し、当該プログラムを管理装置に供給するプログラム格納媒体において、

上記プログラムは、

各種機器が接続される上記管理装置に接続された着脱自在な所定のデータ格納装置の記録媒体から所定のコンテンツデータを再生して取り込む取込ステップと

上記コンテンツデータの各種機器への移動を上記データ格納装置に代えて管理する移動管理ステップとを具える。

238. 請求の範囲第237項に記載のプログラム格納媒体において、

上記プログラムの上記取込ステップは、上記データ格納装置の上記記録媒体から所定のコンテンツ鍵で暗号化されている上記コンテンツデータと、当該コンテンツ鍵と、当該コンテンツ鍵の使用条件を規定した取扱方針に基づいて生成された上記コンテンツデータの利用権を規定し、当該コンテンツデータの保持者を識別するための識別情報を格納した使用許諾条件情報とを取り込み、

上記移動管理ステップは、上記使用許諾条件情報を上記識別情報を変更して更新し、当該更新した上記使用許諾条件情報と共に、上記コンテンツ鍵で暗号化されている上記コンテンツデータと、当該コンテンツ鍵とを上記各種機器へ移動させる。

239. 請求の範囲第237項に記載のプログラム格納媒体において、

上記プログラムの上記取込ステップは、上記各種機器から上記使用許諾条件情報に基づいて返還される当該使用許諾条件情報と、上記コンテンツ鍵で暗号化されている上記コンテンツデータと、当該コンテンツ鍵とを取り込む。

240. 請求の範囲第238項に記載のプログラム格納媒体において、

上記プログラムの上記取込ステップは、上記データ格納装置固有の上記識別情報が格納された上記使用許諾条件情報を取り込み、

上記管理移動ステップは、上記使用許諾条件情報内の上記データ格納装置固有の上記識別情報を上記管理装置固有の上記識別情報に変更して上記使用許諾条件情報を更新する。

2 4 1. 請求の範囲第 2 4 0 項に記載のプログラム格納媒体において、

上記プログラムの上記取込ステップは、上記データ格納装置から上記取扱方針及び上記コンテンツデータの価格情報に基づいて生成された上記コンテンツデータの購入に対する課金情報を取り込む。

2 4 2. 請求の範囲第 2 4 1 項に記載のプログラム格納媒体において、

上記プログラムは、

上記管理装置と上記データ格納装置との間で共有化した一時鍵で暗号化されている所定のデータを当該一時鍵で復号化する復号ステップを具え、

上記取込ステップは、上記データ格納装置から上記一時鍵で暗号化されている上記コンテンツ鍵と、当該一時鍵で暗号化されている上記課金情報とを取り込み、

上記復号ステップは、上記一時鍵で暗号化されている上記コンテンツ鍵と、上記課金情報とをそれぞれ上記一時鍵で復号化する。

2 4 3. 請求の範囲第 2 4 2 項に記載のプログラム格納媒体において、

上記プログラムは、

所定のデータに付加された署名データを検証して上記データの改竄の有無を検出する検出ステップを具え、

上記取込ステップは、上記データ格納装置から上記一時鍵で暗号化された後、署名データが付加された上記課金情報を取り込み、

上記検出ステップは、上記一時鍵で暗号化された上記課金情報に付加されている上記署名を検証する。

2 4 4. 所定のプログラムを格納し、当該プログラムをデータ格納装置に供給するプログラム格納媒体において、

上記プログラムは、



所定の記録装置から着脱自在な上記データ格納装置に送信された所定のコンテンツ鍵で暗号化されているコンテンツデータと、当該コンテンツ鍵と、当該コンテンツ鍵の使用条件を規定した取扱方針と受信する受信ステップと、

上記記録装置の制御のもとに、上記取扱方針に基づいて上記コンテンツデータの利用権を規定し、当該コンテンツデータの保持者を識別するための識別情報を格納した使用許諾条件情報を作成する情報作成ステップと、

上記記録装置の制御のもとに、上記使用許諾条件情報と、上記コンテンツ鍵で暗号化されている上記コンテンツデータ及び当該コンテンツ鍵並びに上記取扱方針とを所定の記録媒体に記録する記録ステップと、

各種機器への上記コンテンツデータの移動を管理する管理装置に上記データ格納装置が接続された際に、当該管理装置の制御のもとに、上記記録媒体から上記コンテンツ鍵で暗号化されている上記コンテンツデータと、当該コンテンツ鍵と、上記使用許諾条件情報とを再生する再生ステップと、

上記管理装置の制御のもとに、上記データ格納装置から上記コンテンツ鍵で暗号化されている上記コンテンツデータ及び当該コンテンツ鍵と共に、上記コンテンツデータを管理するための上記使用許諾条件情報を上記管理装置に送信して上記コンテンツデータの管理を移行する送信ステップとを具える。

245. 請求の範囲第244項に記載のプログラム格納媒体において、

上記プログラムの上記情報作成ステップは、上記取扱方針に基づいて、上記コンテンツデータの利用権を規定し、当該コンテンツデータの保持者を識別するための変更可能な識別情報を格納した使用許諾条件情報を作成する。

246. 請求の範囲第245項に記載のプログラム格納媒体において、

上記プログラムの上記情報作成ステップは、上記データ格納装置固有の上記識別情報が格納された上記使用許諾条件情報を作成する。

247. 請求の範囲第246項に記載のプログラム格納媒体において、

上記プログラムの上記受信ステップは、上記記録装置から上記コンテンツ鍵で暗号化されているコンテンツデータと、当該コンテンツ鍵と、上記取扱方針と共に送信された上記コンテンツデータの価格情報を受信し、

上記情報作成ステップは、上記取扱方針及び上記価格情報に基づいて上記コンテンツデータの購入に対する課金情報を作成し所定のメモリに記録する。

248. 請求の範囲第247項に記載のプログラム格納媒体において、

上記プログラムの上記情報作成ステップは、耐タンパ性を有する上記メモリに上記課金情報を記録する。

249. 請求の範囲第248項に記載のプログラム格納媒体において、

上記プログラムは、

上記管理装置との間で共有化した一時鍵で上記コンテンツ鍵を暗号化すると共に、当該一時鍵で上記課金情報を暗号化する暗号化ステップを具え、

上記送信ステップは、上記コンテンツ鍵で暗号化されている上記コンテンツデータ及び上記使用許諾条件情報と共に、上記一時鍵で暗号化した上記コンテンツ鍵と、上記一時鍵で暗号化した上記課金情報とを上記管理装置に送信する。

250. 請求の範囲第249項に記載のプログラム格納媒体において、

上記プログラムは、

上記一時鍵で暗号化された上記課金情報に、改竄の有無を検証するための署名データを付加する付加ステップを具え、

上記送信ステップは、上記コンテンツ鍵で暗号化されている上記コンテンツデータ、上記使用許諾条件情報及び上記一時鍵で暗号化した上記コンテンツ鍵と共に上記一時鍵で暗号化して署名データが付加された上記課金情報を上記管理装置に送信する。

251. 情報受信装置と上記規制装置とから構築される情報提供システムにおいて、

上記情報受信装置は、

所定のコンテンツデータを受信する受信装置側受信手段と、

上記受信したコンテンツデータを示す利用許可データに署名を付加する付加手段と、

上記署名を付加した上記利用許可データを送信する受信装置側送信手段とを具備し、

上記情報規制装置は、

上記署名の付加された上記利用許可データを受信する規制装置側受信手段と、

上記利用可能データに付加された上記署名を検証して、当該利用許可データが不当なデータであるか否かを判断する判断手段と、

上記署名の検証の結果、上記利用許可データが不当なデータであると判断したときには、上記情報受信装置に上記コンテンツデータの利用の不許可を通知し、上記情報受信装置に対して上記コンテンツデータの利用を禁止する通知手段とを具備する。

252. 請求の範囲第251項に記載の情報提供システムにおいて、

上記情報規制装置の上記判断手段は、上記利用許可データの署名を検証して、当該利用許可データが上記情報受信装置が受信した上記コンテンツデータとは異なる他のコンテンツデータを示すように改竄されているときに、上記利用許可データを不当なデータであると判断する。

253. 請求の範囲第252項に記載の情報提供システムにおいて、

上記情報受信装置の上記付加手段は、上記コンテンツデータの利用権を規定した上記利用許可データに上記署名を付加し、

上記情報規制装置の上記判断手段は、上記利用許可データの署名を検証して、

当該利用許可データの規定する上記利用権が他の利用権を規定するように改竄されているときには、上記利用許可データを不当なデータであると判断する。

2 5 4. 請求の範囲第 2 5 3 項に記載の情報提供システムにおいて、

上記コンテンツデータを送信する情報送信装置を具え、

上記情報受信装置と、上記情報規制装置とは、上記情報送信装置を介してオンライン接続される。

2 5 5. 所定の情報受信装置とオンライン接続された情報規制装置において、

上記情報受信装置から送信される、所定のコンテンツデータを示し、かつ署名が付加された利用許可データを受信する受信手段と、

上記利用許可データの署名を検証して、当該利用許可データが不当なデータであるか否かを判断する判断手段と、

上記署名の検証の結果、上記利用許可データが不当なデータであると判断したときには、上記情報受信装置に上記コンテンツデータの利用の不許可を通知し、上記情報受信装置に対して上記コンテンツデータの利用を禁止する通知手段とを具える。

2 5 6. 請求の範囲第 2 5 5 項に記載の情報規制装置において、

上記判断手段は、上記利用許可データの署名を検証して、当該利用許可データが上記情報受信装置が受信した上記コンテンツデータとは異なる他のコンテンツデータを示すように改竄されているときに、上記利用許可データを不当なデータであると判断する。

2 5 7. 請求の範囲第 2 5 6 項に記載の情報規制装置において、

上記受信手段は、上記コンテンツデータの利用権を規定して上記署名の付加された上記利用許可データを受信し、

上記判断手段は、上記利用許可データの署名を検証して、上記利用権が他の利用権を規定するように改竄されているときには、上記利用許可データを不当なデータであると判断する。

258. 請求の範囲第255項に記載の情報規制装置において、

上記受信手段は、上記利用許可データとして、上記コンテンツデータの購入処理途中に生成されて上記署名が付加された課金情報を受信し、

上記判断手段は、上記課金情報の署名を検証して、上記当該課金情報が不当なデータであるか否かを判断し、

上記通知手段は、上記署名の検証の結果、上記課金情報が改竄されていることにより不当なデータであると判断したときには、上記情報受信装置に上記コンテンツデータの利用の不許可として購入処理の中断を通知し、上記情報受信装置に対して上記コンテンツデータの購入を禁止する。

259. 請求の範囲第258項に記載の情報規制装置において、

暗号化されている所定のデータを復号化する復号手段を具え、

上記受信手段は、上記情報規制装置と上記情報受信装置との間で共有化した一時鍵で暗号化された後に上記署名が付加された上記課金情報を受信し、

上記判断手段は、上記課金情報の署名を検証して、上記当該課金情報が不当なデータであるか否かを判断し、

上記復号手段は、上記署名の検証の結果、上記課金情報が正当なデータであると判断されたときに上記暗号化されている上記課金情報を上記一時鍵で復号化する。

260. 所定の情報規制装置にオンライン接続された情報受信装置において、

送信される所定のコンテンツデータを受信する受信手段と、

上記コンテンツデータを示す利用許可データに、当該利用許可データの示す上

記コンテンツデータが他のコンテンツデータに改竄されたか否かを検出し得る署名を付加する付加手段と、

上記署名を付加した上記利用許可データを上記署名の検証結果に応じて上記コンテンツデータの利用の禁止の有無を決定する上記情報規制装置に送信する送信手段とを具える。

261. 請求の範囲第260項に記載の情報受信装置において、

上記付加手段は、上記コンテンツデータの利用権を規定した上記利用許可データが、他の利用権を規定するように改竄されているか否かを検出し得るようにするために上記署名を付加する。

262. 請求の範囲第260項に記載の情報受信装置において、

上記コンテンツデータの購入処理を実行して上記コンテンツデータの購入に対する課金情報を生成する購入処理手段を具え、

上記付加手段は、上記利用許可データとして、上記コンテンツデータの購入処理途中に生成された上記課金情報に上記署名を付加する。

263. 請求の範囲第262項に記載の情報受信装置において、

上記情報規制装置から上記コンテンツデータの利用の禁止の有無の通知を受け取る受取手段を具え、

上記購入処理手段は、上記コンテンツデータの購入処理途中に上記情報受信装置から上記コンテンツデータの利用の不許可が通知されると、上記購入処理を中断する。

264. 請求の範囲第263項に記載の情報受信装置において、

上記情報規制装置との間で共有化された一時鍵で上記課金情報を暗号化する暗号化手段を具え、

上記付加手段は、上記暗号化された上記課金情報に上記署名を付加する。

265. 請求の範囲第260項に記載の情報受信装置において、

上記コンテンツデータを送信する所定の情報送信装置を介して上記情報規制装置にオンライン接続される接続手段を具える。

266. 情報提供方法において、

情報受信装置により、所定のコンテンツデータを受信し、当該受信したコンテンツデータを示す利用許可データに署名を付加して送信する送信ステップと、

情報規制装置より、上記利用許可データの署名を検証して、当該利用許可データが不当なデータであるか否かを判断し、当該不当なデータであると判断したときには、上記情報受信装置に対して上記コンテンツデータの利用を禁止する利用禁止ステップとを具える。

267. 請求の範囲第266項に記載の情報提供方法において、

上記利用禁止ステップは、上記利用許可データの署名を検証して、当該利用許可データが上記情報受信装置の受信した上記コンテンツデータとは異なる他のコンテンツデータを示すように改竄されているときに、上記利用許可データを不当なデータであると判断する。

268. 請求の範囲第267項に記載の情報提供方法において、

上記送信ステップは、上記コンテンツデータの利用権を規定した上記利用許可データに上記署名を付加して送信し、

上記利用禁止ステップは、上記利用許可データの署名を検証して、当該利用許可データの規定する上記利用権が他の利用権を規定するように改竄されているときには、上記不当なデータであると判断する。

269. 請求の範囲第268項に記載の情報提供方法において、

上記送信ステップは、上記情報受信装置が、上記コンテンツデータを送信する情報送信装置を介してオンライン接続された上記情報規制装置に上記利用許可データを送信する。

270. 所定の情報受信装置とオンライン接続された情報規制装置による情報規制方法において、

上記情報受信装置から送信される、所定のコンテンツデータを示し、かつ署名が付加された利用許可データを受信する受信ステップと、

上記利用許可データの署名を検証して、当該利用許可データが不当なデータであるか否かを判断する判断ステップと、

上記署名の検証の結果、上記利用許可データが不当なデータであると判断したときには、上記情報受信装置に上記コンテンツデータの利用の不許可を通知し、上記情報受信装置に対して上記コンテンツデータの利用を禁止する通知ステップとを具える。

271. 請求の範囲第270項に記載の情報規制方法において、

上記判断ステップは、上記利用許可データの署名を検証して、当該利用許可データが上記情報受信装置が受信した上記コンテンツデータとは異なる他のコンテンツデータを示すように改竄されているときに、上記利用許可データを不当なデータであると判断する。

272. 請求の範囲第271項に記載の情報規制方法において、

上記受信ステップは、上記コンテンツデータの利用権を規定して上記署名の付加された上記利用許可データを受信し、

上記判断ステップは、上記利用許可データの署名を検証して、上記利用権が他の利用権を規定するように改竄されているときには、上記利用許可データを不当



なデータであると判断する。

273. 請求の範囲第270項に記載の情報規制方法において、

上記受信ステップは、上記利用許可データとして、上記コンテンツデータの購入処理途中に生成されて上記署名が付加された課金情報を受信し、

上記判断ステップは、上記課金情報の署名を検証して、上記当該課金情報が不当なデータであるか否かを判断し、

上記通知ステップは、上記署名の検証の結果、上記課金情報が改竄されていることにより不当なデータであると判断したときには、上記情報受信装置に上記コンテンツデータの利用の不許可として購入処理の中断を通知して上記情報受信装置に対して上記コンテンツデータの購入を禁止する。

274. 請求の範囲第273項に記載の情報規制方法において、

暗号化されている所定のデータを復号化する復号ステップを具え、

上記受信ステップは、上記情報規制装置と上記情報受信装置との間で共有化した一時鍵で暗号化された後に上記署名が付加された上記課金情報を受信し、

上記判断ステップは、上記課金情報の署名を検証して、上記当該課金情報が不当なデータであるか否かを判断し、

上記復号ステップは、上記署名の検証の結果、上記課金情報が正当なデータであると判断されたときに上記暗号化されている上記課金情報を上記一時鍵で復号化する。

275. 所定の情報規制装置にオンライン接続された情報受信装置で所定のコンテンツデータを利用するデータ利用方法において、

送信される所定のコンテンツデータを受信する受信ステップと、

上記コンテンツデータを示す利用許可データに、当該利用許可データの示す上記コンテンツデータが他のコンテンツデータに改竄されたか否かを検出し得る署

名を付加する付加ステップと、

上記署名を付加した上記利用許可データを上記署名の検証結果に応じて上記コンテンツデータの利用の禁止の有無を決定する上記情報規制装置に送信する送信ステップとを具える。

276. 請求の範囲第275項に記載のデータ利用方法において、

上記付加ステップは、上記コンテンツデータの利用権を規定した上記利用許可データが、他の利用権を規定するように改竄されているか否かを検出し得るようにするために上記署名を付加する。

277. 請求の範囲第275項に記載のデータ利用方法において、

上記コンテンツデータの購入処理を実行して上記コンテンツデータの購入に対する課金情報を生成する購入処理ステップを具え、

上記付加ステップは、上記利用許可データとして、上記コンテンツデータの購入処理途中に生成された上記課金情報に上記署名を付加する。

278. 請求の範囲第277項に記載のデータ利用方法において、

上記情報規制装置から上記コンテンツデータの利用の禁止の有無の通知を受け取る受取ステップを具え、

上記購入処理ステップは、上記コンテンツデータの購入処理途中に上記情報受信装置から上記コンテンツデータの利用の不許可が通知されると、上記購入処理を中断する。

279. 請求の範囲第278項に記載のデータ利用方法において、

上記情報規制装置との間で共有化された一時鍵で上記課金情報を暗号化する暗号化ステップを具え、

上記付加ステップは、上記暗号化された上記課金情報に上記署名を付加する。

280. 請求の範囲第275項に記載のデータ利用方法において、

上記コンテンツデータを送信する所定の情報送信装置を介して上記情報規制装置にオンライン接続される接続ステップを具える。

281. 所定のプログラムを格納し、当該プログラムを情報規制装置に供給するプログラム格納媒体において、

上記プログラムは、

オンライン接続された上記情報受信装置から送信される、所定のコンテンツデータを示し、かつ署名が付加された利用許可データを受信する受信ステップと、

上記利用許可データの署名を検証して、当該利用許可データが不当なデータであるか否かを判断する判断ステップと、

上記署名の検証の結果、上記利用許可データが不当なデータであると判断したときには、上記情報受信装置に上記コンテンツデータの利用の不許可を通知し、上記情報受信装置に対して上記コンテンツデータの利用を禁止する通知ステップとを具える。

282. 請求の範囲第281項に記載のプログラム格納媒体において、

上記プログラムの上記判断ステップは、上記利用許可データの署名を検証して、当該利用許可データが上記情報受信装置が受信した上記コンテンツデータとは異なる他のコンテンツデータを示すように改竄されているときに、上記利用許可データを不当なデータであると判断する。

283. 請求の範囲第282項に記載のプログラム格納媒体において、

上記プログラムの上記受信ステップは、上記コンテンツデータの利用権を規定して上記署名の付加された上記利用許可データを受信し、

上記判断ステップは、上記利用許可データの署名を検証して、上記利用権が他の利用権を規定するように改竄されているときには、上記利用許可データを不当

なデータであると判断する。

284. 請求の範囲第281項に記載のプログラム格納媒体において、

上記プログラムの上記受信ステップは、上記利用許可データとして、上記コンテンツデータの購入処理途中に生成されて上記署名が付加された課金情報を受信し、

上記判断ステップは、上記課金情報の署名を検証して、上記当該課金情報が不当なデータであるか否かを判断し、

上記通知ステップは、上記署名の検証の結果、上記課金情報が改竄されていることにより不当なデータであると判断したときには、上記情報受信装置に上記コンテンツデータの利用の不許可として購入処理の中断を通知して上記情報受信装置に対して上記コンテンツデータの購入を禁止する。

285. 請求の範囲第284項に記載のプログラム格納媒体において、

上記プログラムは、

暗号化されている所定のデータを復号化する復号ステップを具え、

上記受信ステップは、上記情報規制装置と上記情報受信装置との間で共有化した一時鍵で暗号化された後に上記署名が付加された上記課金情報を受信し、

上記判断ステップは、上記課金情報の署名を検証して、上記当該課金情報が不当なデータであるか否かを判断し、

上記復号ステップは、上記署名の検証の結果、上記課金情報が正当なデータであると判断されたときに上記暗号化されている上記課金情報を上記一時鍵で復号化する。

286. 所定のプログラムを格納し、当該プログラムを情報受信装置に供給するプログラム格納媒体において、

上記プログラムは、

所定の情報規制装置にオンライン接続された情報受信装置で所定のコンテンツデータを受信する受信ステップと、

上記コンテンツデータを示す利用許可データに、当該利用許可データの示す上記コンテンツデータが他のコンテンツデータに改竄されたか否かを検出し得る署名を付加する付加ステップと、

上記署名を付加した上記利用許可データを上記署名の検証結果に応じて上記コンテンツデータの利用の禁止の有無を決定する上記情報規制装置に送信する送信ステップとを具える。

287. 請求の範囲第286項に記載のプログラム格納媒体において、

上記プログラムの上記付加ステップは、上記コンテンツデータの利用権を規定した上記利用許可データが、他の利用権を規定するように改竄されているか否かを検出し得るようにするために上記署名を付加する。

288. 請求の範囲第286項に記載のプログラム格納媒体において、

上記プログラムは、

上記コンテンツデータの購入処理を実行して上記コンテンツデータの購入に対する課金情報を生成する購入処理ステップを具え、

上記付加ステップは、上記利用許可データとして、上記コンテンツデータの購入処理途中に生成された上記課金情報に上記署名を付加する。

289. 請求の範囲第288項に記載のプログラム格納媒体において、

上記プログラムは、

上記情報規制装置から上記コンテンツデータの利用の禁止の有無の通知を受け取る受取ステップを具え、

上記購入処理ステップは、上記コンテンツデータの購入処理途中に上記情報受信装置から上記コンテンツデータの利用の不許可が通知されると、上記購入処理

を中断する。

290. 請求の範囲第289項に記載のプログラム格納媒体において、  
上記プログラムは、  
上記情報規制装置との間で共有化された一時鍵で上記課金情報を暗号化する暗号化ステップを具え、  
上記付加ステップは、上記暗号化された上記課金情報に上記署名を付加する。

291. 請求の範囲第286項に記載のプログラム格納媒体において、  
上記プログラムは、  
上記コンテンツデータを送信する所定の情報送信装置を介して上記情報規制装置にオンライン接続される接続ステップを具える。

292. 情報送信装置から送信される所定のコンテンツデータを情報提供装置に提供する情報提供システムにおいて、

上記情報送信装置は、  
上記コンテンツデータを所定のコンテンツ鍵で暗号化する暗号化手段と、  
上記コンテンツ鍵及び当該コンテンツ鍵で暗号化された上記コンテンツデータを送信する送信手段とを具え、

上記情報提供装置は、  
上記情報送信装置から送信される上記コンテンツ鍵及び当該コンテンツ鍵で暗号化された上記コンテンツデータを受信する受信手段と、

上記コンテンツ鍵で暗号化された上記コンテンツデータを当該コンテンツ鍵で復号化する復号化手段と、

上記コンテンツ鍵で復号化した上記コンテンツデータに所定の情報を電子透かしにより挿入する電子透かし挿入手段と、

上記情報を挿入した上記コンテンツデータを着脱自在な記録媒体に記録するデ

ータ記録手段とを具える。

293. 請求の範囲第292項に記載の情報提供システムにおいて、

上記情報提供装置の上記電子透かし挿入手段は、上記コンテンツデータに複製制限用の上記情報を上記電子透かしにより挿入する。

294. 請求の範囲第292項に記載の情報提供システムにおいて、

上記情報送信装置は、

上記コンテンツ鍵の使用条件を規定した取扱方針を生成する取扱方針生成手段を具え、

上記送信手段は、上記コンテンツ鍵及び当該コンテンツ鍵で暗号化された上記コンテンツデータと共に、上記取扱方針を送信し、

上記情報提供装置は、

上記取扱方針に基づいて、上記コンテンツデータの利用権を規定した使用許諾条件情報を作成する使用許諾条件情報作成手段と、

上記コンテンツ鍵及び当該コンテンツ鍵で暗号化された上記コンテンツデータと共に、上記使用許諾条件情報を着脱自在な所定のデータ格納装置に送信して格納する格納手段とを具える。

295. 請求の範囲第294項に記載の情報提供システムにおいて、

上記情報提供装置の上記格納手段は、上記コンテンツ鍵及び当該コンテンツ鍵で暗号化された上記コンテンツデータと共に、上記取扱方針を上記データ格納装置に送信して格納する共に、上記データ格納装置により上記取扱方針に基づいて上記使用許諾条件情報を作成して格納する。

296. 請求の範囲第295項に記載の情報提供システムにおいて、

上記情報送信装置から上記情報提供装置への上記コンテンツデータの送信を管

理する管理装置を具え、

上記情報提供装置の上記格納手段は、上記データ格納装置を識別するための識別情報を上記管理装置に送信し、

上記管理装置は、上記識別情報に基づいて、上記コンテンツデータを格納した上記データ格納装置を管理する。

297. 情報送信装置から送信された所定のコンテンツデータを提供する情報提供装置において、

上記情報送信装置から送信される所定のコンテンツ鍵で暗号化された上記コンテンツデータと、当該コンテンツ鍵とを受信する受信手段と、

上記コンテンツ鍵で暗号化された上記コンテンツデータを当該コンテンツ鍵で復号化する復号化手段と、

上記コンテンツ鍵で復号化した上記コンテンツデータに所定の情報を電子透かしにより挿入する電子透かし挿入手段と、

上記情報を挿入した上記コンテンツデータを着脱自在な記録媒体に記録するデータ記録手段とを具える。

298. 請求の範囲第297項に記載の情報提供装置において、

上記電子透かし挿入手段は、上記コンテンツデータに複製制限用の上記情報を上記電子透かしにより挿入する。

299. 請求の範囲第297項に記載の情報提供装置において、

上記情報送信装置から上記コンテンツ鍵及び当該コンテンツ鍵で暗号化された上記コンテンツデータと共に送信される、上記コンテンツ鍵の使用条件を規定した取扱方針に基づいて、上記コンテンツデータの使用条件を規定した使用許諾条件情報を作成する使用許諾条件情報作成手段と、

上記コンテンツ鍵及び当該コンテンツ鍵で暗号化された上記コンテンツデータ



と共に、上記使用許諾条件情報を着脱自在な所定のデータ格納装置に送信して格納する格納手段とを具える。

300. 請求の範囲第299項に記載の情報提供装置において、

上記格納手段は、上記コンテンツ鍵及び当該コンテンツ鍵で暗号化された上記コンテンツデータと、上記取扱方針とを上記データ格納装置に送信して格納すると共に、上記データ格納装置により上記取扱方針に基づいて上記使用許諾条件情報を作成して格納する。

301. 情報送信装置から送信された所定のコンテンツデータを提供する情報提供装置において、

上記情報送信装置から上記コンテンツ鍵及び当該コンテンツ鍵で暗号化された上記コンテンツデータと共に送信される、上記コンテンツ鍵の使用条件を規定した取扱方針に基づいて、上記コンテンツデータの使用条件を規定した使用許諾条件情報を作成する使用許諾条件情報作成手段と、

上記コンテンツ鍵及び当該コンテンツ鍵で暗号化された上記コンテンツデータと共に、上記使用許諾条件情報を着脱自在な所定のデータ格納装置に送信して格納する格納手段とを具える。

302. 請求の範囲第301項に記載の情報提供装置において、

上記格納手段は、上記コンテンツ鍵及び当該コンテンツ鍵で暗号化された上記コンテンツデータと、上記取扱方針とを上記データ格納装置に送信して格納すると共に、上記データ格納装置により上記取扱方針に基づいて上記使用許諾条件情報を作成して格納する。

303. 情報提供装置から送信される所定のコンテンツデータを格納する着脱自在なデータ格納装置において、

所定の記録媒体と、

上記情報提供装置から送信された、上記コンテンツ鍵及び当該コンテンツ鍵で暗号化された上記コンテンツデータと、上記コンテンツ鍵の使用条件を規定した取扱方針に基づいて必要に応じて作成された上記コンテンツデータの使用条件を規定した使用許諾条件情報とを受信する受信手段と、

上記コンテンツ鍵及び当該コンテンツ鍵で暗号化された上記コンテンツデータと、上記使用許諾条件情報とを上記記録媒体に記録する記録手段とを具える。

304. 請求の範囲第303項に記載のデータ格納装置において、

上記情報提供装置から送信される上記取扱方針に基づいて、上記使用許諾条件情報を作成する使用許諾条件情報作成手段を具え、

上記記録手段は、上記情報提供装置から上記コンテンツ鍵及び当該コンテンツ鍵で暗号化された上記コンテンツデータと、上記取扱方針が送信されたとき、上記コンテンツ鍵及び当該コンテンツ鍵で暗号化された上記コンテンツデータと、上記使用許諾条件情報作成手段により作成された上記使用許諾条件情報を上記記録媒体に記録する。

305. 情報送信装置から送信される所定のコンテンツデータを情報提供装置に提供する情報提供方法において、

上記情報送信装置により所定のコンテンツ鍵と、当該コンテンツ鍵で暗号化した上記コンテンツデータとを送信するデータ送信ステップと、

上記情報提供装置により上記コンテンツ鍵及び当該コンテンツ鍵で暗号化された上記コンテンツデータを受信する受信ステップと、

上記情報提供装置により上記コンテンツ鍵で暗号化された上記コンテンツデータを当該コンテンツ鍵で復号化する復号化ステップと、

上記情報提供装置により上記コンテンツ鍵で復号化した上記コンテンツデータに所定の情報を電子透かしにより挿入する電子透かし挿入ステップと、

上記情報提供装置により上記情報を挿入した上記コンテンツデータを着脱自在な記録媒体に記録するデータ記録ステップとを具える。

306. 請求の範囲第305項に記載の情報提供方法において、

上記電子透かし挿入ステップは、上記コンテンツデータに複製制限用の上記情報を上記電子透かしにより挿入する。

307. 請求の範囲第305項に記載の情報提供方法において、

上記情報送信装置により上記情報提供装置に送信するための上記コンテンツ鍵の使用条件を規定した取扱方針を生成する取扱方針生成ステップと、

上記情報提供装置により上記取扱方針に基づいて、上記コンテンツデータの利用権を規定した使用許諾条件情報を作成する使用許諾条件情報作成ステップと、

上記情報提供装置により上記コンテンツ鍵及び当該コンテンツ鍵で暗号化された上記コンテンツデータと共に、上記使用許諾条件情報を着脱自在な所定のデータ格納装置に送信して格納する格納ステップとを具える。

308. 請求の範囲第307項に記載の情報提供方法において、

上記格納ステップは、上記コンテンツ鍵及び当該コンテンツ鍵で暗号化された上記コンテンツデータと共に、上記取扱方針を上記データ格納装置に送信して格納する共に、上記データ格納装置により上記取扱方針に基づいて上記使用許諾条件情報を作成して格納する。

309. 請求の範囲第308項に記載の情報提供方法において、

上記情報提供装置により、上記情報送信装置から上記情報提供装置への上記コンテンツデータの送信を管理する管理装置に上記データ格納装置を識別するための識別情報を送信する識別情報送信ステップと、

上記管理装置により上記識別情報に基づいて、上記コンテンツデータを格納し

た上記データ格納装置を管理する管理ステップとを具える。

310. 情報提供装置により所定のコンテンツデータを提供する情報提供方法において、

情報送信装置から送信される所定のコンテンツ鍵で暗号化された上記コンテンツデータと、当該コンテンツ鍵とを受信する受信ステップと、

上記コンテンツ鍵で暗号化された上記コンテンツデータを当該コンテンツ鍵で復号化する復号化ステップと、

上記コンテンツ鍵で復号化した上記コンテンツデータに所定の情報を電子透かしにより挿入する電子透かし挿入ステップと、

上記情報を挿入した上記コンテンツデータを着脱自在な記録媒体に記録するデータ記録ステップとを具える。

311. 請求の範囲第310項に記載の情報提供方法において、

上記電子透かし挿入ステップは、上記コンテンツデータに複製制限用の上記情報を上記電子透かしにより挿入する。

312. 請求の範囲第310項に記載の情報提供方法において、

上記情報送信装置から上記コンテンツ鍵及び当該コンテンツ鍵で暗号化された上記コンテンツデータと共に送信される、上記コンテンツ鍵の使用条件を規定した取扱方針に基づいて、上記コンテンツデータの使用条件を規定した使用許諾条件情報を作成する使用許諾条件情報作成ステップと、

上記コンテンツ鍵及び当該コンテンツ鍵で暗号化された上記コンテンツデータと共に、上記使用許諾条件情報を着脱自在な所定のデータ格納装置に送信して格納する格納ステップとを具える。

313. 請求の範囲第312項に記載の情報提供方法において、

上記格納ステップは、上記コンテンツ鍵及び当該コンテンツ鍵で暗号化された上記コンテンツデータと、上記取扱方針とを上記データ格納装置に送信して格納すると共に、上記データ格納装置により上記取扱方針に基づいて上記使用許諾条件情報を作成して格納する。

314. 情報提供装置により所定のコンテンツデータを提供する情報提供方法において、

情報送信装置から上記コンテンツ鍵及び当該コンテンツ鍵で暗号化された上記コンテンツデータと共に送信される、上記コンテンツ鍵の使用条件を規定した取扱方針に基づいて、上記コンテンツデータの使用条件を規定した使用許諾条件情報を作成する使用許諾条件情報作成ステップと、

上記コンテンツ鍵及び当該コンテンツ鍵で暗号化された上記コンテンツデータと共に、上記使用許諾条件情報を着脱自在な所定のデータ格納装置に送信して格納する格納ステップとを具える。

315. 請求の範囲第314項に記載の情報提供方法において、

上記格納ステップは、上記コンテンツ鍵及び当該コンテンツ鍵で暗号化された上記コンテンツデータと、上記取扱方針とを上記データ格納装置に送信して格納すると共に、上記データ格納装置により上記取扱方針に基づいて上記使用許諾条件情報を作成して格納する。

316. 情報提供装置から送信される所定のコンテンツデータを着脱自在なデータ格納装置に格納するデータ格納方法において、

上記情報提供装置から送信された上記コンテンツ鍵及び当該コンテンツ鍵で暗号化された上記コンテンツデータと、上記コンテンツ鍵の使用条件を規定した取扱方針に基づいて必要に応じて作成された上記コンテンツデータの使用条件を規定した使用許諾条件情報とを受信する受信ステップと、

上記コンテンツ鍵及び当該コンテンツ鍵で暗号化された上記コンテンツデータと、上記使用許諾条件情報とを記録媒体に記録する記録ステップとを具える。

317. 請求の範囲第316項に記載のデータ格納方法において、

上記情報提供装置から送信される上記取扱方針に基づいて、上記使用許諾条件情報を作成する使用許諾条件情報作成ステップを具え、

上記記録ステップは、上記情報提供装置から上記コンテンツ鍵及び当該コンテンツ鍵で暗号化された上記コンテンツデータと、上記取扱方針のみが送信されたとき、上記コンテンツ鍵及び当該コンテンツ鍵で暗号化された上記コンテンツデータと、上記使用許諾条件情報作成ステップにより作成された上記使用許諾条件情報を上記記録媒体に記録する。

318. 所定のプログラムを格納し、当該プログラムを情報提供装置に供給するプログラム格納媒体において、

上記プログラムは、

情報送信装置から送信される所定のコンテンツ鍵で暗号化されたコンテンツデータと、当該コンテンツ鍵とを受信する受信ステップと、

上記コンテンツ鍵で暗号化された上記コンテンツデータを当該コンテンツ鍵で復号化する復号化ステップと、

上記コンテンツ鍵で復号化した上記コンテンツデータに所定の情報を電子透かしにより挿入する電子透かし挿入ステップと、

上記情報を挿入した上記コンテンツデータを着脱自在な記録媒体に記録するデータ記録ステップとを具える。

319. 請求の範囲第318項に記載のプログラム格納媒体において、

上記プログラムの上記電子透かし挿入ステップは、上記コンテンツデータに複製制限用の上記情報を上記電子透かしにより挿入する。

320. 請求の範囲第318項に記載のプログラム格納媒体において、

上記プログラムは、

上記情報送信装置から上記コンテンツ鍵及び当該コンテンツ鍵で暗号化された上記コンテンツデータと共に送信される、上記コンテンツ鍵の使用条件を規定した取扱方針に基づいて、上記コンテンツデータの使用条件を規定した使用許諾条件情報を作成する使用許諾条件情報作成ステップと、

上記コンテンツ鍵及び当該コンテンツ鍵で暗号化された上記コンテンツデータと共に、上記使用許諾条件情報を着脱自在な所定のデータ格納装置に送信して格納する格納ステップとを具える。

321. 請求の範囲第320項に記載のプログラム格納媒体において、

上記プログラムの上記格納ステップは、上記コンテンツ鍵及び当該コンテンツ鍵で暗号化された上記コンテンツデータと、上記取扱方針とを上記データ格納装置に送信して格納すると共に、上記データ格納装置により上記取扱方針に基づいて上記使用許諾条件情報を作成して格納する。

322. 所定のプログラムを格納し、当該プログラムを情報提供装置に供給するプログラム格納媒体において、

上記プログラムは、

情報送信装置から所定のコンテンツ鍵及び当該コンテンツ鍵で暗号化されたコンテンツデータと共に送信される、上記コンテンツ鍵の使用条件を規定した取扱方針に基づいて、上記コンテンツデータの使用条件を規定した使用許諾条件情報を作成する使用許諾条件情報作成ステップと、

上記コンテンツ鍵及び当該コンテンツ鍵で暗号化された上記コンテンツデータと共に、上記使用許諾条件情報を着脱自在な所定のデータ格納装置に送信して格納する格納ステップとを具える。

3 2 3. 請求の範囲第 3 2 2 項に記載のプログラム格納媒体において、

上記プログラムの上記格納ステップは、上記コンテンツ鍵及び当該コンテンツ鍵で暗号化された上記コンテンツデータと、上記取扱方針とを上記データ格納装置に送信して格納すると共に、上記データ格納装置により上記取扱方針に基づいて上記使用許諾条件情報を作成して格納する。

3 2 4. 所定のプログラムを格納し、当該プログラムをデータ格納装置に供給するプログラム格納媒体において、

上記プログラムは、

上記情報提供装置から着脱自在な上記データ格納装置に送信された上記コンテンツ鍵及び当該コンテンツ鍵で暗号化された上記コンテンツデータと、上記コンテンツ鍵の使用条件を規定した取扱方針に基づいて必要に応じて作成された上記コンテンツデータの使用条件を規定した使用許諾条件情報とを受信する受信ステップと、

上記コンテンツ鍵及び当該コンテンツ鍵で暗号化された上記コンテンツデータと、上記使用許諾条件情報とを記録媒体に記録する記録ステップとを具える。

3 2 5. 請求の範囲第 3 2 4 項に記載のプログラム格納媒体において、

上記プログラムは、

上記情報提供装置から送信される上記取扱方針に基づいて、上記使用許諾条件情報を作成する使用許諾条件情報作成ステップを具え、

上記記録ステップは、上記情報提供装置から上記コンテンツ鍵及び当該コンテンツ鍵で暗号化された上記コンテンツデータと、上記取扱方針のみが送信されたとき、上記コンテンツ鍵及び当該コンテンツ鍵で暗号化された上記コンテンツデータと、上記使用許諾条件情報作成ステップにより作成された上記使用許諾条件情報を上記記録媒体に記録する。



3 2 6. 所定のコンテンツデータを所定のデータ格納装置に格納する情報記録装置において、

複数の上記コンテンツデータを保持するコンテンツサーバと、

上記コンテンツサーバに保持した各上記コンテンツデータをカテゴリ分けして管理し、所望する上記カテゴリ及びコンテンツ数が指定されると、当該指定された上記カテゴリに属する各上記コンテンツデータのなかから、上記指定された上記コンテンツ数分の複数の上記コンテンツデータを任意に選定する選定手段と、

上記選定された各上記コンテンツデータを上記コンテンツサーバから読み出して上記データ格納装置に格納する格納手段とを具える。

3 2 7. 請求の範囲第 3 2 6 項に記載の情報記録装置において、

上記指定された上記コンテンツ数に基づいて、乱数を発生する乱数発生手段を具え、

上記選定手段は、上記乱数を用いて、各上記コンテンツデータを選定する。

3 2 8. 請求の範囲第 3 2 7 項に記載の情報記録装置において、

上記選定手段により選定された各上記コンテンツデータの利用権を規定した使用許諾条件情報を作成する使用許諾条件情報作成手段を具え、

上記格納手段は、各上記コンテンツデータと共に上記使用許諾条件情報を上記データ格納装置に格納する。

3 2 9. 請求の範囲第 3 2 8 項に記載の情報記録装置において、

上記使用許諾条件情報作成手段は、各上記コンテンツデータの再生回数を制限するように上記利用権を規定した上記使用許諾条件情報を作成する。

3 3 0. 請求の範囲第 3 2 8 項に記載の情報記録装置において、

上記使用許諾条件情報作成手段は、各上記コンテンツデータの再生期間を制限

するように上記利用権を規定した上記使用許諾条件情報を作成する。

3 3 1. 請求の範囲第 3 2 8 項に記載の情報記録装置において、

上記使用許諾条件情報作成手段は、所定の識別情報を格納するようにして上記使用許諾条件情報を作成し、

上記格納手段は、上記使用許諾条件情報に格納された上記識別情報に基づいて、削除対象の上記コンテンツデータを検出し、当該検出した上記コンテンツデータに上書きするように、新たな上記コンテンツデータを格納する。

3 3 2. 情報記録装置により所定のコンテンツデータが格納されるデータ格納装置において、

所定の記録媒体と、

上記情報記録装置から送信された、カテゴリ分けされた複数の上記コンテンツデータのなかの所望する上記カテゴリに属し、かつ所望するコンテンツ数分の複数の上記コンテンツデータを受信するコンテンツ受信手段と、

各上記コンテンツデータを上記記録媒体に一括して記録する記録手段とを具える。

3 3 3. 請求の範囲第 3 3 2 項に記載のデータ格納装置において、

上記記録手段は、上記情報記録装置から各上記コンテンツデータと共に、当該各上記コンテンツデータの利用権を規定した使用許諾条件情報が送信されることにより、各上記コンテンツデータと上記使用許諾条件情報とを上記記録媒体に記録する。

3 3 4. 請求の範囲第 3 3 3 項に記載のデータ格納装置において、

上記記録手段は、各上記コンテンツデータと共に、各上記コンテンツデータの再生回数を制限するように上記利用権を規定した上記使用許諾条件情報を上記記

録媒体に記録する。

335. 請求の範囲第333項に記載のデータ格納装置において、

上記記録手段は、各上記コンテンツデータと共に、各上記コンテンツデータの再生期間を制限するように上記利用権を規定した上記使用許諾条件情報を上記記録媒体に記録する。

336. 情報記録装置によりデータ格納装置に所定のコンテンツデータを格納するデータ格納方法において、

予めコンテンツサーバに保持している複数の上記コンテンツサーバをカテゴリ分けして管理し、所望する上記カテゴリ及びコンテンツ数が指定されると、当該指定された上記カテゴリに属する各上記コンテンツデータのなかから、上記指定された上記コンテンツ数分の複数の上記コンテンツデータを任意に選定する選定ステップと、

上記選定された各上記コンテンツデータを上記コンテンツサーバから読み出して上記データ格納装置に格納する格納ステップとを具える。

337. 請求の範囲第336項に記載のデータ格納方法において、

上記指定された上記コンテンツ数に基づいて、乱数を発生する乱数発生ステップを具え、

上記選定ステップは、上記乱数を用いて、各上記コンテンツデータを選定する。

338. 請求の範囲第337項に記載のデータ格納方法において、

上記選定ステップにより選定された各上記コンテンツデータの利用権を規定した使用許諾条件情報を作成する使用許諾条件情報作成ステップを具え、

上記格納ステップは、各上記コンテンツデータと共に上記使用許諾条件情報を

上記データ格納装置に格納する。

339. 請求の範囲第338項に記載のデータ格納方法において、

上記使用許諾条件情報作成ステップは、各上記コンテンツデータの再生回数を制限するように上記利用権を規定した上記使用許諾条件情報を作成する。

340. 請求の範囲第338項に記載のデータ格納方法において、

上記使用許諾条件情報作成ステップは、各上記コンテンツデータの再生期間を制限するように上記利用権を規定した上記使用許諾条件情報を作成する。

341. 請求の範囲第338項に記載のデータ格納方法において、

上記使用許諾条件情報作成ステップは、所定の識別情報を格納するようにして上記使用許諾条件情報を作成し、

上記格納ステップは、上記使用許諾条件情報に格納された上記識別情報に基づいて、削除対象の上記コンテンツデータを検出し、当該検出した上記コンテンツデータに上書きするように、新たな上記コンテンツデータを格納する。

342. 情報記録装置によりデータ格納装置に所定のコンテンツデータを格納するデータ格納方法において、

上記情報記録装置から上記データ格納装置に送信された、カテゴリ分けされた複数の上記コンテンツデータのなかの所望する上記カテゴリに属し、かつ所望するコンテンツ数分の複数の上記コンテンツデータを受信するコンテンツ受信ステップと、

各上記コンテンツデータを上記データ格納装置内の記録媒体に一括して記録する記録ステップとを具える。

343. 請求の範囲第342項に記載のデータ格納方法において、

上記記録ステップは、上記情報記録装置から各上記コンテンツデータと共に、当該各上記コンテンツデータの利用権を規定した使用許諾条件情報が送信されることにより、各上記コンテンツデータと上記使用許諾条件情報とを上記記録媒体に記録する。

344. 請求の範囲第343項に記載のデータ格納方法において、

上記記録ステップは、各上記コンテンツデータと共に、各上記コンテンツデータの再生回数を制限するように上記利用権を規定した上記使用許諾条件情報を上記記録媒体に記録する。

345. 請求の範囲第343項に記載のデータ格納方法において、

上記記録ステップは、各上記コンテンツデータと共に、各上記コンテンツデータの再生期間を制限するように上記利用権を規定した上記使用許諾条件情報を上記記録媒体に記録する。

346. 所定のプログラムを格納し、当該プログラムを情報記録装置に供給するプログラム格納媒体において、

上記プログラムは、

予めコンテンツサーバに保持している複数のコンテンツサーバをカテゴリ分けして管理し、所望する上記カテゴリ及びコンテンツ数が指定されると、当該指定された上記カテゴリに属する各上記コンテンツデータのなかから、上記指定された上記コンテンツ数分の複数の上記コンテンツデータを任意に選定する選定ステップと、

上記選定された各上記コンテンツデータを上記コンテンツサーバから読み出して上記データ格納装置に格納する格納ステップとを具える。

347. 請求の範囲第346項に記載のプログラム格納媒体において、

上記プログラムは、  
上記指定された上記コンテンツ数に基づいて、乱数を発生する乱数発生ステップを具え、  
上記選定ステップは、上記乱数を用いて、各上記コンテンツデータを選定する。

348. 請求の範囲第347項に記載のプログラム格納媒体において、  
上記プログラムは、  
上記選定ステップにより選定された各上記コンテンツデータの利用権を規定した使用許諾条件情報を作成する使用許諾条件情報作成ステップを具え、  
上記格納ステップは、各上記コンテンツデータと共に上記使用許諾条件情報を上記データ格納装置に格納する。

349. 請求の範囲第348項に記載のプログラム格納媒体において、  
上記プログラムの上記使用許諾条件情報作成ステップは、各上記コンテンツデータの再生回数を制限するように上記利用権を規定した上記使用許諾条件情報を作成する。

350. 請求の範囲第348項に記載のプログラム格納媒体において、  
上記プログラムの上記使用許諾条件情報作成ステップは、各上記コンテンツデータの再生期間を制限するように上記利用権を規定した上記使用許諾条件情報を作成する。

351. 請求の範囲第348項に記載のプログラム格納媒体において、  
上記プログラムの上記使用許諾条件情報作成ステップは、所定の識別情報を格納するようにして上記使用許諾条件情報を作成し、  
上記格納ステップは、上記使用許諾条件情報に格納された上記識別情報に基づ

いて、削除対象の上記コンテンツデータを検出し、当該検出した上記コンテンツデータに上書きするように、新たな上記コンテンツデータを格納する。

352. 所定のプログラムを格納し、当該プログラムをデータ格納装置に供給するプログラム格納媒体において、

上記プログラムは、

情報記録装置から送信された、カテゴリ分けされた複数のコンテンツデータのなかの所望する上記カテゴリに属し、かつ所望するコンテンツ数分の複数の上記コンテンツデータを受信するコンテンツ受信ステップと、

各上記コンテンツデータを記録媒体に一括して記録する記録ステップとを具える。

353. 請求の範囲第352項に記載のプログラム格納媒体において、

上記プログラムの上記記録ステップは、上記情報記録装置から各上記コンテンツデータと共に、当該各上記コンテンツデータの利用権を規定した使用許諾条件情報が送信されることにより、各上記コンテンツデータと上記使用許諾条件情報とを上記記録媒体に記録する。

354. 請求の範囲第353項に記載のプログラム格納媒体において、

上記プログラムの上記記録ステップは、各上記コンテンツデータと共に、各上記コンテンツデータの再生回数を制限するように上記利用権を規定した上記使用許諾条件情報を上記記録媒体に記録する。

355. 請求の範囲第353項に記載のプログラム格納媒体において、

上記プログラムの上記記録ステップは、各上記コンテンツデータと共に、各上記コンテンツデータの再生期間を制限するように上記利用権を規定した上記使用許諾条件情報を上記記録媒体に記録する。

3 5 6. 情報送信装置、情報受信装置及びリスト送信装置から構築される情報提供システムにおいて、

上記情報送信装置は、

所定のコンテンツデータを送信するデータ送信手段を具え、

上記リスト送信装置は、

提供禁止対象に指定された上記コンテンツデータを示す提供禁止リストを作成するリスト作成手段と、

上記提供禁止リストを送信するリスト送信手段とを具え、

上記情報受信装置は、

上記コンテンツデータ及び上記提供禁止リストを受信する受信手段と、

上記提供禁止リストに基づいて、上記情報送信装置から送信される上記コンテンツデータが上記提供禁止対象であるか否かを判別する判別手段と、

上記判別手段から得られる判別結果に応じて上記コンテンツデータが上記提供禁止対象である場合には、当該コンテンツデータの取り込みを中止する取込中止手段とを具える。

3 5 7. 請求の範囲第3 5 6項に記載の情報提供システムにおいて、

上記リスト送信装置は、上記提供禁止リストに利用禁止対象に指定された上記情報送信装置を登録する登録手段を具え、

上記情報受信装置の上記判別手段は、上記提供禁止リストに基づいて、上記情報送信装置から送信される上記コンテンツデータが上記提供禁止対象であるか否かを判別すると共に、上記情報送信装置が上記利用禁止対象であるか否かを判別し、

上記取込中止手段は、上記判別手段から得られる判別結果に応じて上記コンテンツデータが上記提供禁止対象である場合と、上記情報送信装置が上記利用禁止対象である場合には、それぞれ上記コンテンツデータの取り込みを中止する。



358. 請求の範囲第357項に記載の情報提供システムにおいて、

上記情報受信装置は、

上記リスト送信装置にオンライン接続され、上記提供禁リストを受信する1又は複数のオンライン機器と、

上記リスト送信装置にオンライン接続されていない1又は複数のオフライン機器とを具え、

上記オンライン機器は、

上記オフライン機器が接続された際に当該オフライン機器に上記提供禁止リストを送信するオンライン機器用リスト送信手段と、

上記情報送信装置から送信される上記コンテンツデータを直接受信し、又は上記情報送信装置から送信される上記コンテンツデータを他の上記オンライン機器及びオフライン機器を介して受信するオンライン機器用受信手段と、

上記提供禁止リストに基づいて、上記コンテンツデータの取り込みを必要に応じて中止するオンライン機器用取込中止手段とを具え、

上記オフライン機器は、

上記オフライン機器が接続された際に当該オフライン機器に必要に応じて上記提供禁止リストを送信するオフライン機器用リスト送信手段と、

上記オンライン機器から送信される上記提供禁止リストを受信すると共に、上記情報送信装置から送信される上記コンテンツデータを直接受信し、又は上記情報送信装置から送信される上記コンテンツデータを他の上記オンライン機器及びオフライン機器を介して受信するオフライン機器用受信手段と、

上記提供禁止リストに基づいて、上記コンテンツデータの取り込みを必要に応じて中止するオフライン機器用取込中止手段とを具える。

359. 請求の範囲第358項に記載の情報提供システムにおいて、

上記オンライン機器は、

上記オフライン機器から送信された上記コンテンツデータを上記オンライン機

器用受信手段が受信すると、上記提供禁止リストに基づいて、上記コンテンツデータが上記提供禁止対象であるか否かを判別すると共に、当該コンテンツデータの提供元である上記情報送信装置が上記利用禁止対象であるか否かを判別するオンライン機器用判別手段を具え、

上記オンライン機器用取込中止手段は、上記オンライン機器用判別手段から得られる判別結果に応じて、上記コンテンツデータが上記提供禁止対象である場合と、上記情報送信装置が上記利用禁止対象である場合には、上記コンテンツデータの取り込みを中止し、

上記オンライン機器用リスト送信手段は、上記コンテンツデータが上記提供禁止対象である場合と、上記情報送信装置が上記利用禁止対象である場合には、上記提供禁止リストを上記オフライン機器に送信する。

360. 請求の範囲第359項に記載の情報提供システムにおいて、

上記オフライン機器は、

他の上記オフライン機器から送信された上記コンテンツデータをオフライン機器用受信手段が受信すると、上記提供禁止リストに基づいて、上記コンテンツデータが上記提供禁止対象であるか否かを判別すると共に、当該コンテンツデータの提供元である上記情報送信装置が上記利用禁止対象であるか否かを判別するオフライン機器用判別手段を具え、

オフライン機器用取込中止手段は、上記オフライン機器用判別手段から得られる判別結果に応じて、上記コンテンツデータが上記提供禁止対象である場合と、上記情報送信装置が上記利用禁止対象である場合には、上記コンテンツデータの取り込みを中止し、

上記オフライン機器用リスト送信手段は、上記コンテンツデータが上記提供禁止対象である場合と、上記情報送信装置が上記利用禁止対象である場合には、上記提供禁止リストを上記他のオフライン機器に送信する。

361. 情報送信装置から送信される所定のコンテンツデータを受信する情報受信装置に所定のリストを送信するリスト送信装置において、

提供禁止対象に指定された上記コンテンツデータを示す提供禁止リストを作成するリスト作成手段と、

上記提供禁止リストを上記情報受信装置に送信する送信手段とを具える。

362. 請求の範囲第361項に記載のリスト送信装置において、

上記リスト作成手段は、上記提供禁止リストに利用禁止対象に指定された上記情報送信装置を登録する。

363. 請求の範囲第362項に記載のリスト送信装置において、

上記リスト作成手段は、上記コンテンツデータが上記提供禁止対象に指定される毎、又は上記情報送信装置が上記利用禁止対象に指定される毎に上記提供禁止リストを更新し、

上記送信手段は、上記提供禁止リストが更新される毎に上記情報受信装置に送信する。

364. 情報送信装置から送信される所定のコンテンツデータと、リスト送信装置から送信される所定のリストを受信する情報受信装置において、

上記リスト送信装置から送信される提供禁止対象に指定された上記コンテンツデータを示す提供禁止リストを受信する受信手段と、

上記提供禁止リストを保持するリスト保持手段と、

上記提供禁止リストに基づいて、上記情報送信装置から送信される上記コンテンツデータが上記提供禁止対象であるか否かを判別する判別手段と、

上記判別手段から得られる判別結果に応じて、上記コンテンツデータが上記提供禁止対象である場合には、当該コンテンツデータの取り込みを中止する取込中止手段とを具える。

3 6 5. 請求の範囲第 3 6 4 項に記載の情報受信装置において、

上記リスト保持手段は、上記リスト送信装置から送信される、上記提供禁止対象に指定された上記コンテンツデータと共に、利用禁止対象に指定された上記情報送信装置を示す上記提供禁止リストを保持し、

上記判別手段は、上記提供禁止リストに基づいて、上記情報送信装置から送信される上記コンテンツデータが上記提供禁止対象であるか否かを判別すると共に、上記情報送信装置が上記利用禁止対象であるか否かを判別し、

上記取込中止手段は、上記コンテンツデータが上記提供禁止対象である場合と、上記情報送信装置が上記利用禁止対象である場合には、それぞれ上記コンテンツデータの取り込みを中止する。

3 6 6. 請求の範囲第 3 6 5 項に記載の情報受信装置において、

上記リスト送信装置にオンライン接続され、上記提供禁止リストを受信する 1 又は複数のオンライン機器と、

上記リスト送信装置にオンライン接続されていない 1 又は複数のオフライン機器とを具え、

上記オンライン機器は、

上記オフライン機器が接続された際に当該オフライン機器に上記提供禁止リストを送信するオンライン機器用リスト送信手段と、

上記情報送信装置から送信される上記コンテンツデータを直接受信し、又は上記情報送信装置から送信される上記コンテンツデータを他の上記オンライン機器及びオフライン機器を介して受信するオンライン機器用受信手段と、

上記提供禁止リストに基づいて、上記コンテンツデータの取り込みを必要に応じて中止するオンライン機器用取込中止手段とを具え、

上記オフライン機器は、

上記オフライン機器が接続された際に当該オフライン機器に必要に応じて上記提供禁止リストを送信するオフライン機器用リスト送信手段と、

上記オンライン機器から送信される上記提供禁止リストを受信すると共に、上記情報送信装置から送信される上記コンテンツデータを直接受信し、又は上記情報送信装置から送信される上記コンテンツデータを他の上記オンライン機器及びオフライン機器を介して受信するオフライン機器用受信手段と、

上記提供禁止リストに基づいて、上記コンテンツデータの取り込みを必要に応じて中止するオフライン機器用取込中止手段とを具える。

367. 請求の範囲第366項に記載の情報受信装置において、

上記オンライン機器は、

上記オフライン機器から送信された上記コンテンツデータを上記オンライン機器用受信手段が受信すると、上記提供禁止リストに基づいて、上記コンテンツデータが上記提供禁止対象であるか否かを判別すると共に、当該コンテンツデータの提供元である上記情報送信装置が上記利用禁止対象であるか否かを判別するオンライン機器用判別手段を具え、

上記オンライン機器用取込中止手段は、上記オンライン機器用判別手段から得られる判別結果に応じて、上記コンテンツデータが上記提供禁止対象である場合と、上記情報送信装置が上記利用禁止対象である場合には、上記コンテンツデータの取り込みを中止し、

上記オンライン機器用リスト送信手段は、上記コンテンツデータが上記提供禁止対象である場合と、上記情報送信装置が上記利用禁止対象である場合には、上記提供禁止リストを上記オフライン機器に送信する。

368. 請求の範囲第367項に記載の情報受信装置において、

上記オフライン機器は、

他の上記オフライン機器から送信された上記コンテンツデータをオフライン機器用受信手段が受信すると、上記提供禁止リストに基づいて、上記コンテンツデータが上記提供禁止対象であるか否かを判別すると共に、当該コンテンツデータ

の提供元である上記情報送信装置が上記利用禁止対象であるか否かを判別するオフライン機器用判別手段を具え、

オフライン機器用取込中止手段は、上記オフライン機器用判別手段から得られる判別結果に応じて、上記コンテンツデータが上記提供禁止対象である場合と、上記情報送信装置が上記利用禁止対象である場合には、上記コンテンツデータの取り込みを中止し、

上記オフライン機器用リスト送信手段は、上記コンテンツデータが上記提供禁止対象である場合と、上記情報送信装置が上記利用禁止対象である場合には、上記提供禁止リストを上記他のオフライン機器に送信する。

### 369. 情報提供方法において、

リスト送信装置により提供禁止対象に指定された上記コンテンツデータを示す提供禁止リストを作成し、当該作成した提供禁止リストを送信すると共に、情報送信装置により所定のコンテンツデータを送信する送信ステップと、

情報受信装置により上記提供禁止リストを受信すると共に、上記コンテンツデータを受信する受信ステップと、

上記情報受信装置により上記提供禁止リストに基づいて、上記情報送信装置から送信される上記コンテンツデータが上記提供禁止対象であるか否かを判別する判別ステップと、

上記判別ステップにより得られた判別結果に応じて、上記コンテンツデータが上記提供禁止対象である場合には、当該コンテンツデータの取り込みを中止する取込中止ステップとを具える。

### 370. 請求の範囲第369項に記載の情報提供方法において、

上記送信ステップは、上記リスト送信装置により上記提供禁止リストに利用禁止対象に指定された上記情報送信装置を登録して送信し、

上記判別ステップは、上記情報受信装置により上記提供禁止リストに基づいて

、上記コンテンツデータが上記提供禁止対象であるか否かを判別すると共に、上記情報送信装置が上記利用禁止対象であるか否かを判別し、

上記取込中止ステップは、上記情報受信装置により上記コンテンツデータが上記提供禁止対象である場合と、上記情報送信装置が上記利用禁止対象である場合には、それぞれ上記コンテンツデータの取り込みを中止する。

### 371. 請求の範囲第370項に記載の情報提供方法において、

上記情報受信装置を構築する、上記リスト送信装置にオンライン接続され、上記提供禁リストを受信する1又は複数のオンライン機器と、上記リスト送信装置にオンライン接続されていない1又は複数のオフライン機器との間で、上記オンライン機器が上記オフライン機器に接続された際に当該オフライン機器に上記提供禁リストを送信する機器間リスト送信ステップと、

上記オンライン機器及びオフライン機器は、上記情報送信装置から送信される上記コンテンツデータを直接受信し、又は上記情報送信装置から送信される上記コンテンツデータを他の上記オンライン機器及びオフライン機器を介して受信し、上記提供禁リストに基づいて、当該コンテンツデータの取り込みを必要に応じて中止する機器取込中止ステップとを具える。

### 372. 請求の範囲第371項に記載の情報提供方法において、

上記オンライン機器が上記オフライン機器から上記コンテンツデータが送信されると、上記提供禁リストに基づいて、上記コンテンツデータが上記提供禁止対象であるか否かを判別すると共に、当該コンテンツデータの提供元である上記情報送信装置が上記利用禁止対象であるか否かを判別する第1の判別ステップと

、  
上記第1の判別ステップにおいて、上記コンテンツデータが上記提供禁止対象である場合と、上記情報送信装置が上記利用禁止対象である場合には、それぞれ上記コンテンツデータの取り込みを中止すると共に、上記提供禁リストを上記

オフライン機器に送信する第 1 の機器間リスト送信ステップとを具える。

3 7 3. 請求の範囲第 3 7 2 項に記載の情報提供方法において、

上記オフライン機器が他の上記オフライン機器から上記コンテンツデータが送信されると、上記提供禁止リストに基づいて、上記コンテンツデータが上記提供禁止対象であるか否かを判別すると共に、当該コンテンツデータの提供元である上記情報送信装置が上記利用禁止対象であるか否かを判別する第 2 の判別ステップと、

上記コンテンツデータが上記提供禁止対象である場合と、上記情報送信装置が上記利用禁止対象である場合には、それぞれ上記コンテンツデータの取り込みを中止すると共に、上記提供禁止リストを上記他のオフライン機器に送信する第 2 の機器間リスト送信ステップとを具える。

3 7 4. 情報送信装置から送信される所定のコンテンツデータを受信する情報受信装置に所定のリストを送信するリスト送信方法において、

提供禁止対象に指定された上記コンテンツデータを示す提供禁止リストを作成するリスト作成ステップと、

上記提供禁止リストを上記情報受信装置に送信する送信ステップとを具える。

3 7 5. 請求の範囲第 3 7 4 項に記載のリスト送信方法において

上記リスト作成ステップは、上記提供禁止リストに利用禁止対象に指定された上記情報送信装置を登録する。

3 7 6. 請求の範囲第 3 7 5 項に記載のリスト送信方法において、

上記リスト作成ステップは、上記コンテンツデータが上記提供禁止対象に指定される毎、又は上記情報送信装置が上記利用禁止対象に指定される毎に上記提供禁止リストを更新し、



上記送信ステップは、上記提供禁止リストが更新される毎に上記情報受信装置に送信する。

377. 情報送信装置から送信される所定のコンテンツデータと、リスト送信装置から送信される所定のリストを受信する情報受信方法において、

上記リスト送信装置から送信される提供禁止対象に指定された上記コンテンツデータを示す提供禁止リストを受信する受信ステップと、

上記提供禁止リストに基づいて、上記情報送信装置から送信される上記コンテンツデータが上記提供禁止対象であるか否かを判別する判別ステップと、

上記判別ステップから得られる判別結果に応じて、上記コンテンツデータが上記提供禁止対象である場合には、当該コンテンツデータの取り込みを中止する取込中止ステップとを具える。

378. 請求の範囲第377項に記載の情報受信方法において、

上記受信ステップは、上記リスト送信装置から送信される、上記提供禁止対象に指定された上記コンテンツデータと共に、利用禁止対象に指定された上記情報送信装置を示す上記提供禁止リストを受信し、

上記判別ステップは、上記提供禁止リストに基づいて、上記情報送信装置から送信される上記コンテンツデータが上記提供禁止対象であるか否かを判別すると共に、上記情報送信装置が上記利用禁止対象であるか否かを判別し、

上記取込中止ステップは、上記コンテンツデータが上記提供禁止対象である場合と、上記情報送信装置が上記利用禁止対象である場合には、それぞれ上記コンテンツデータの取り込みを中止する。

379. 上記リスト送信装置にオンライン接続されたオンライン機器による情報受信方法において、

上記リスト送信装置から送信される上記提供禁止リストを受信すると共に、上記

情報送信装置から送信される上記コンテンツデータを直接受信し、又は上記情報送信装置から送信される上記コンテンツデータを他の上記オンライン機器又は上記リスト送信装置にオンライン接続されていないオフライン機器を介して受信するオンライン機器受信ステップと、

上記オフライン機器が接続された際に当該オフライン機器に上記提供禁止リストを送信するオンライン機器送信ステップとを具える。

380. 請求の範囲第379項に記載の情報受信方法において、

上記提供禁止リストに基づいて、上記コンテンツデータが上記提供禁止対象であるか否かを判別すると共に、上記情報送信装置が上記利用禁止対象であるか否かを判別するオンライン機器判別ステップと、

上記コンテンツデータが上記提供禁止対象である場合と、上記情報送信装置が上記利用禁止対象である場合には、それぞれ上記コンテンツデータの取り込みを中止するオンライン機器取込中止ステップとを具える。

381. 請求の範囲第380項に記載の情報受信方法において、

上記オンライン機器送信ステップは、上記オフライン機器から送信された上記コンテンツデータを受信しているときに、当該コンテンツデータが上記提供禁止対象である場合と、上記情報送信装置が上記利用禁止対象である場合には、上記提供禁止リストを上記オフライン機器に送信する。

382. リスト送信装置にオンライン接続されていないオフライン機器による情報受信方法において、

上記リスト送信装置にオンライン接続されているオンライン機器が接続された際に当該オンライン機器から送信される上記提供禁止リストを受信すると共に、上記情報送信装置から送信される上記コンテンツデータを直接受信し、又は上記情報送信装置から送信される上記コンテンツデータを他の上記オンライン機器又

は上記オフライン機器を介して受信するオフライン機器受信ステップと、

他の上記オフライン機器が接続された際に当該他のオフライン機器に必要な応じて上記提供禁止リストを送信するオフライン機器送信ステップとを具える。

383. 請求の範囲第382項に記載の情報受信方法において、

上記提供禁止リストに基づいて、上記コンテンツデータが上記提供禁止対象であるか否かを判別すると共に、上記情報送信装置が上記利用禁止対象であるか否かを判別するオフライン機器判別ステップと、

上記コンテンツデータが上記提供禁止対象である場合と、上記情報送信装置が上記利用禁止対象である場合には、それぞれ上記コンテンツデータの取り込みを中止するオフライン機器取込中止ステップとを具える。

384. 請求の範囲第383項に記載の情報受信方法において、

上記オフライン送信ステップは、他の上記オフライン機器から送信された上記コンテンツデータを受信しているときに、上記コンテンツデータが上記提供禁止対象である場合と、上記情報送信装置が上記利用禁止対象である場合には、上記提供禁止リストを上記他のオフライン機器に送信する。

385. 所定のプログラムを格納し、当該プログラムをリスト送信装置に供給するプログラム格納媒体において、

上記プログラムは、

提供禁止対象に指定された所定のコンテンツデータを示す提供禁止リストを作成するリスト作成ステップと、

上記提供禁止リストを上記コンテンツデータを受信する情報受信装置に送信する送信ステップとを具える。

386. 請求の範囲第385項に記載のプログラム格納媒体において、

上記プログラムの上記リスト作成ステップは、上記コンテンツデータを上記情報受信装置に送信する情報送信装置のうち、上記提供禁止リストに利用禁止対象に指定された上記情報送信装置を登録する。

387. 請求の範囲第386項に記載のプログラム格納媒体において、

上記プログラムの上記リスト作成ステップは、上記コンテンツデータが上記提供禁止対象に指定される毎、又は上記情報送信装置が上記利用禁止対象に指定される毎に上記提供禁止リストを更新し、

上記送信ステップは、上記提供禁止リストが更新される毎に上記情報受信装置に送信する。

388. 所定のプログラムを格納し、当該プログラムを情報受信装置に供給するプログラム格納媒体において、

上記プログラムは、

リスト送信装置から送信される提供禁止対象に指定された所定のコンテンツデータを示す提供禁止リストを受信する受信ステップと、

上記提供禁止リストに基づいて、情報送信装置から送信される上記コンテンツデータが上記提供禁止対象であるか否かを判別する判別ステップと、

上記判別ステップから得られる判別結果に応じて、上記コンテンツデータが上記提供禁止対象である場合には、当該コンテンツデータの取り込みを中止する取込中止ステップとを具える。

389. 請求の範囲第388項に記載のプログラム格納媒体において、

上記プログラムの上記受信ステップは、上記リスト送信装置から送信される、上記提供禁止対象に指定された上記コンテンツデータと共に、利用禁止対象に指定された上記情報送信装置を示す上記提供禁止リストを受信し、

上記判別ステップは、上記提供禁止リストに基づいて、上記情報送信装置から

送信される上記コンテンツデータが上記提供禁止対象であるか否かを判別すると共に、上記情報送信装置が上記利用禁止対象であるか否かを判別し、

上記取込中止ステップは、上記コンテンツデータが上記提供禁止対象である場合と、上記情報送信装置が上記利用禁止対象である場合には、それぞれ上記コンテンツデータの取り込みを中止する。

390. 所定のプログラムを格納し、当該プログラムをオンライン機器に供給するプログラム格納媒体において、

上記プログラムは、

上記リスト送信装置から送信される上記提供禁リストを受信すると共に、上記情報送信装置から送信される上記コンテンツデータを直接受信し、又は上記情報送信装置から送信される上記コンテンツデータをリスト送信装置にオンライン接続されている他のオンライン機器又は上記リスト送信装置にオンライン接続されていないオフライン機器を介して受信するオンライン機器受信ステップと、

上記オフライン機器が接続された際に当該オフライン機器に上記提供禁止リストを送信するオンライン機器送信ステップとを具える。

391. 請求の範囲第390項に記載のプログラム格納媒体において、

上記プログラムは、

上記提供禁止リストに基づいて、上記コンテンツデータが上記提供禁止対象であるか否かを判別すると共に、上記情報送信装置が上記利用禁止対象であるか否かを判別するオンライン機器判別ステップと、

上記コンテンツデータが上記提供禁止対象である場合と、上記情報送信装置が上記利用禁止対象である場合には、それぞれ上記コンテンツデータの取り込みを中止するオンライン機器取込中止ステップとを具える。

392. 請求の範囲第391項に記載のプログラム格納媒体において、

上記プログラムの上記オンライン機器送信ステップは、上記オフライン機器から送信された上記コンテンツデータを受信しているときに、当該コンテンツデータが上記提供禁止対象である場合と、上記情報送信装置が上記利用禁止対象である場合には、上記提供禁止リストを上記オフライン機器に送信する。

393. 所定のプログラムを格納し、当該プログラムをオフライン機器に供給するプログラム格納媒体において、

上記プログラムは、

リスト送信装置にオンライン接続されているオンライン機器が接続された際に当該オンライン機器から送信される上記提供禁止リストを受信すると共に、上記情報送信装置から送信される上記コンテンツデータを直接受信し、又は上記情報送信装置から送信される上記コンテンツデータを他の上記オンライン機器又は上記リスト送信装置にオンライン接続されていないオフライン機器を介して受信するオフライン機器受信ステップと、

他の上記オフライン機器が接続された際に当該他のオフライン機器に必要な応じて上記提供禁止リストを送信するオフライン機器送信ステップとを具える。

394. 請求の範囲第393項に記載のプログラム格納媒体において、

上記プログラムは、

上記提供禁止リストに基づいて、上記コンテンツデータが上記提供禁止対象であるか否かを判別すると共に、上記情報送信装置が上記利用禁止対象であるか否かを判別するオフライン機器判別ステップと、

上記コンテンツデータが上記提供禁止対象である場合と、上記情報送信装置が上記利用禁止対象である場合には、それぞれ上記コンテンツデータの取り込みを中止するオフライン機器取込中止ステップとを具える。

395. 請求の範囲第394項に記載のプログラム格納媒体において、

上記プログラムの上記オフライン送信ステップは、他の上記オフライン機器から送信された上記コンテンツデータを受信しているときに、上記コンテンツデータが上記提供禁止対象である場合と、上記情報送信装置が上記利用禁止対象である場合には、上記提供禁止リストを上記他のオフライン機器に送信する。

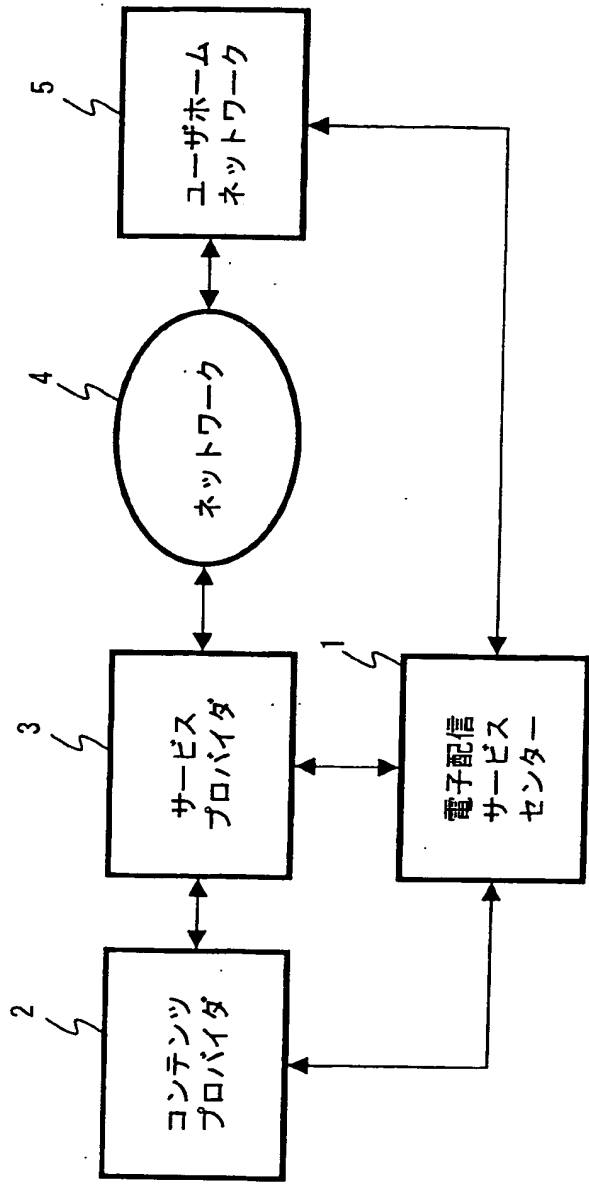
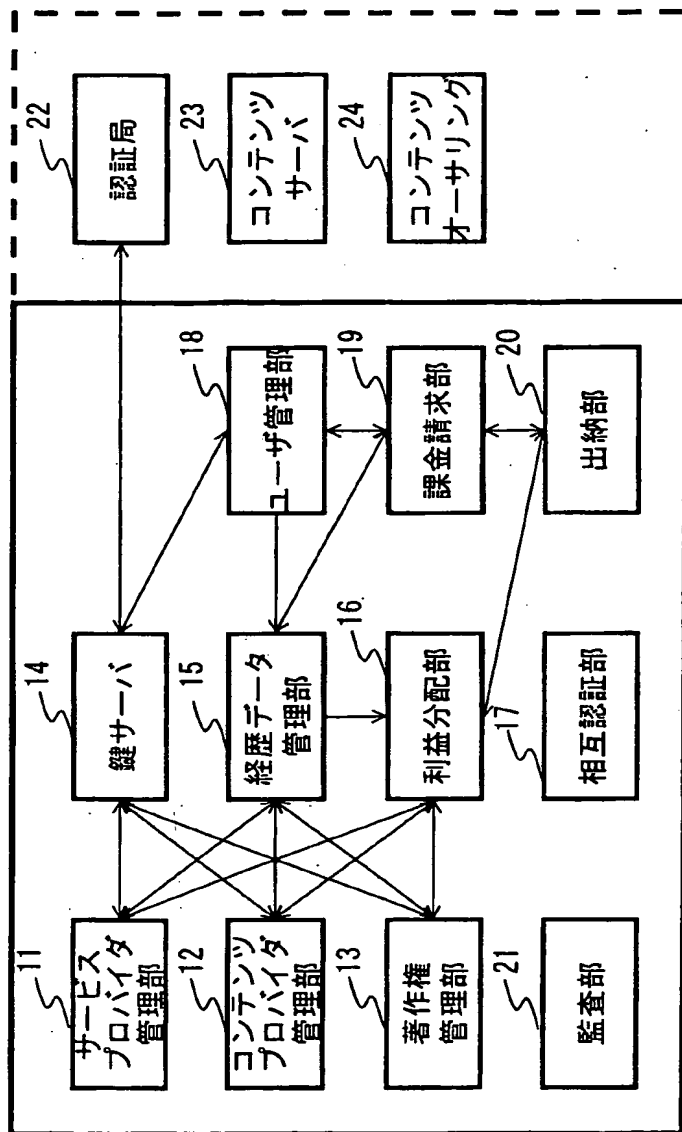


図 1





電子配信サービスセンタ  
から切り離されるモデルも、  
一緒のモデルも考えられる

図 2

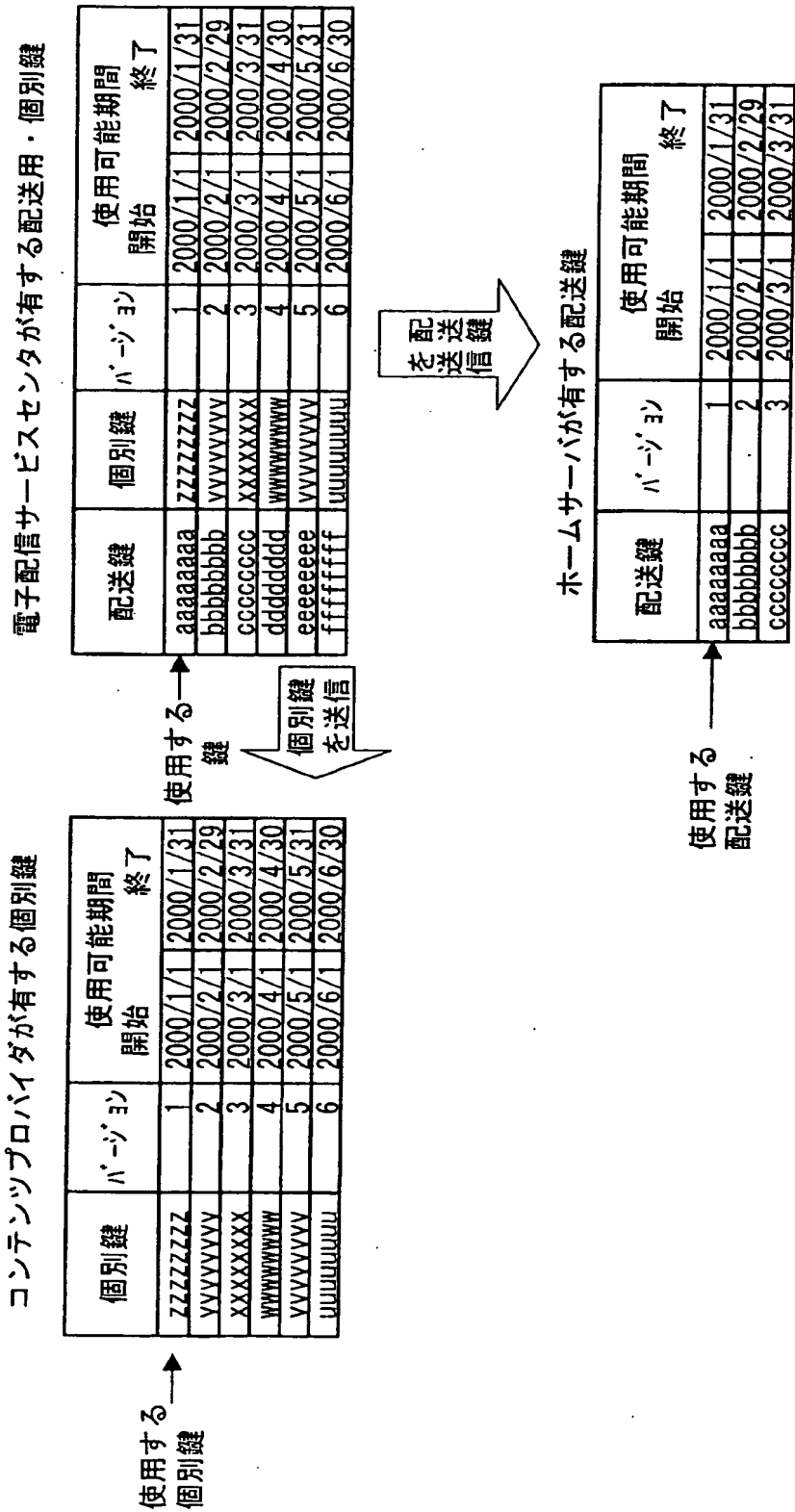


図 3

電子配信サービスセンタが有する配送用・個別鍵

配送鍵	個別鍵	パージン	使用可能期間 開始 終了
aaaaaaa	zzzzzzz	1	2000/1/1 2000/1/31
bbbbbbb	vvvvvvv	2	2000/2/1 2000/2/29
ccccccc	xxxxxxx	3	2000/3/1 2000/3/31
ddddddd	wwwwwww	4	2000/4/1 2000/4/30
eeeeeee	vvvvvvv	5	2000/5/1 2000/5/31
fffffff	uuuuuuu	6	2000/6/1 2000/6/30
ggggggg	ttttttt	7	2000/7/1 2000/7/31

使用する  
鍵

個別鍵  
を送信



コンテンツプロバイダが有する個別鍵

個別鍵	パージン	使用可能期間 開始 終了
vvvvvvvv	2	2000/2/1 2000/2/29
xxxxxxx	3	2000/3/1 2000/3/31
wwwwwww	4	2000/4/1 2000/4/30
vvvvvvvv	5	2000/5/1 2000/5/31
uuuuuuu	6	2000/6/1 2000/6/30
ttttttt	7	2000/7/1 2000/7/31

使用する  
個別鍵

ホームサーバが有する配送鍵

配送鍵	パージン	使用可能期間 開始 終了
bbbbbbb	2	2000/2/1 2000/2/29
ccccccc	3	2000/3/1 2000/3/31
ddddddd	4	2000/4/1 2000/4/30

使用する  
配送鍵

図 4

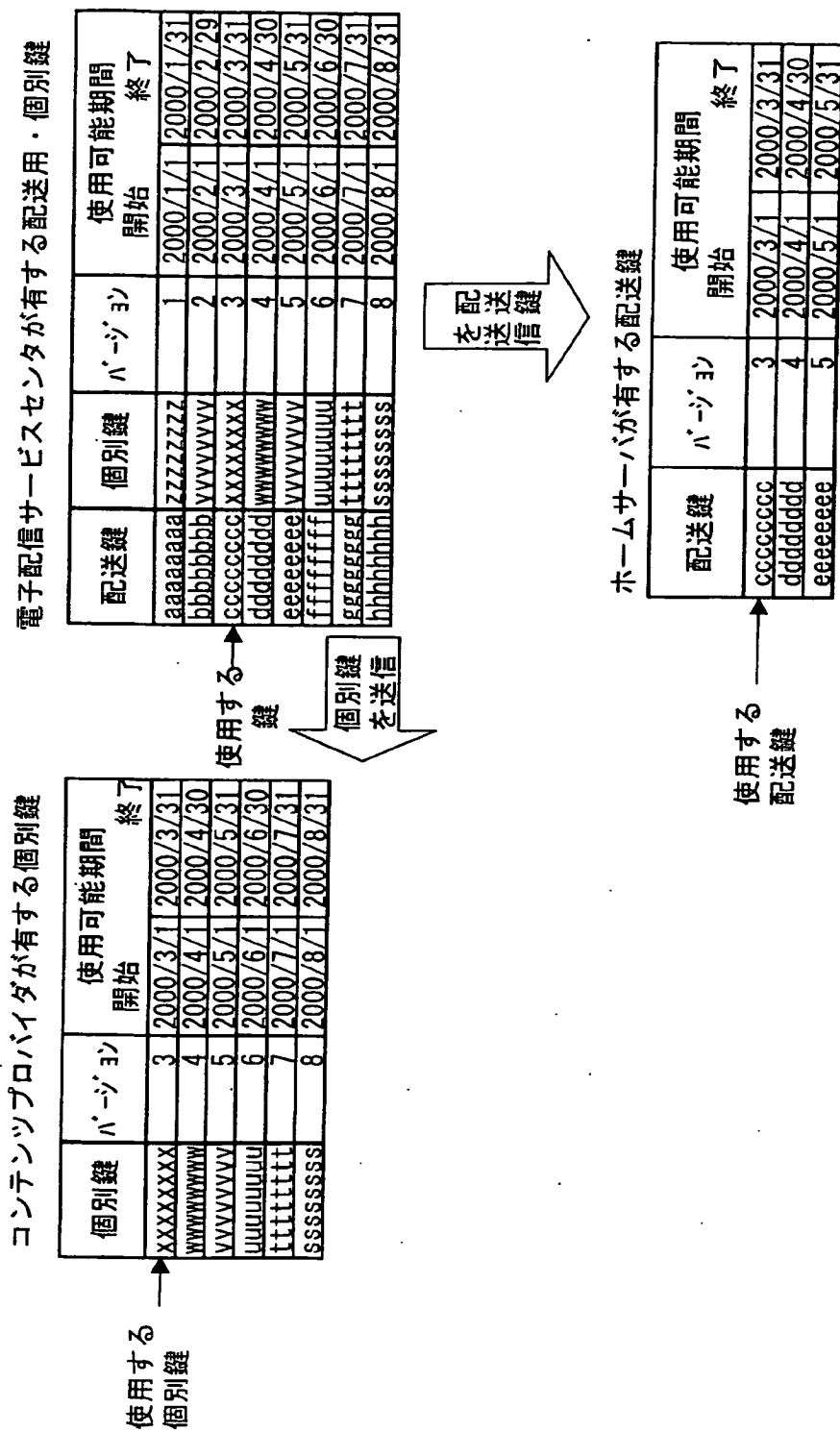


図5

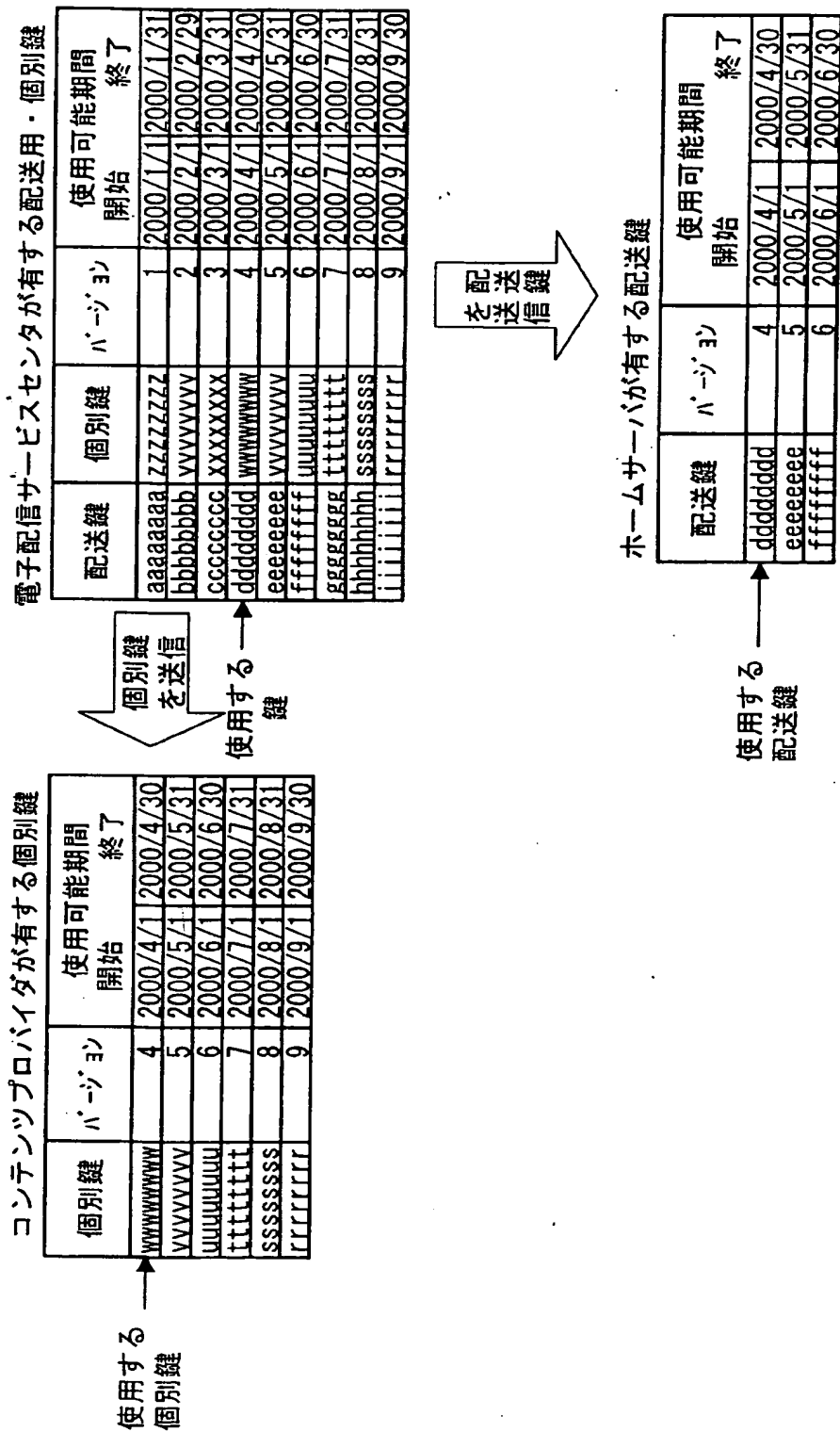


図 6

グループID	ID	サービスセンタとの接続	決済処理	購入処理	代理決済者	代理購入者	登録
GpID1	ID1	可	可	可	—	—	可
	ID2	可	不可	可	ID1	—	可
	ID3	可	不可	可	ID1	—	不可
	ID4	不可	不可	不可	—	ID1	可
	ID5	不可	不可	不可	—	ID2	不可
GpID2	ID6	可	可	可	—	—	不可
	ID7	可	不可	可	ID6	—	不可
	ID8	可	不可	可	ID6	—	可
	ID9	不可	不可	不可	—	ID6.7.8	不可
	ID10	不可	不可	不可	—	ID6.7.8	可
GpID3	ID11	可	可	可	—	—	不可
	ID12	可	不可	可	ID11	—	不可
	ID13	可	不可	可	ID11	—	可
	ID14	不可	不可	不可	—	ID11.12.13	不可
	ID15	不可	不可	不可	—	ID11	可

図 7

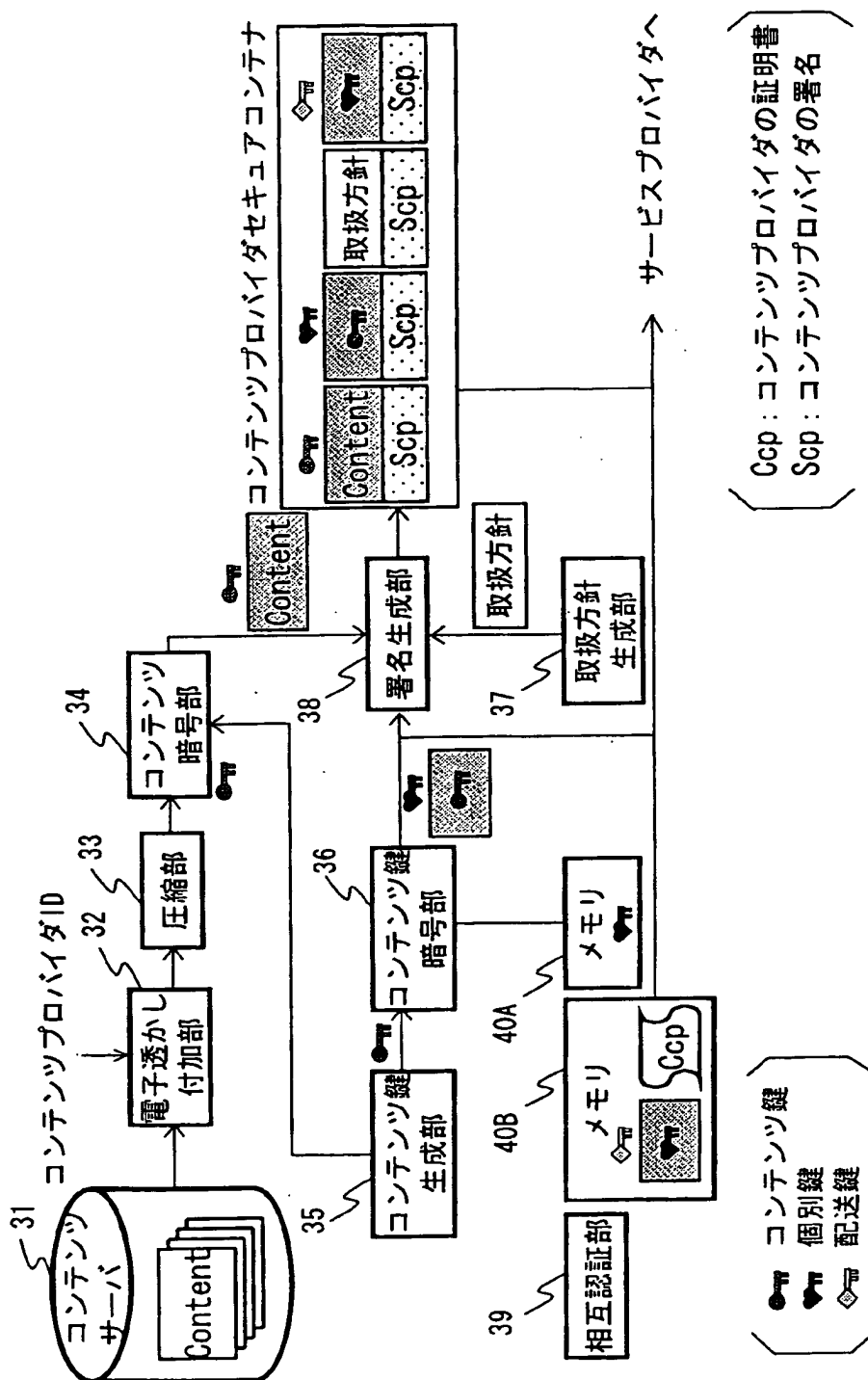
グループID	ID	サービスセタとの接続	決済処理	決済ID	購入処理	代理決済者	代理購入者	登録	署名
GpID1	ID1	可	可	決済ID1	可	—	—	可	署名
	ID2	可	不可	—	可	ID1	—	可	
	ID3	可	不可	—	可	ID1	—	不可	
	ID4	不可	不可	—	不可	—	ID1	可	
	ID5	不可	不可	—	不可	—	ID2	不可	

(A)

グループID	ID	サービスセタとの接続	決済処理	決済ID	購入処理	代理決済者	代理購入者	登録	署名
GpID2	ID6	可	可	決済ID2	可	—	—	可	署名
	ID7	可	不可	—	可	ID6	—	可	
	ID8	可	不可	—	可	ID6	—	不可	
	ID9	不可	不可	—	不可	—	ID6.7.8	可	
	ID10	不可	不可	—	不可	—	ID6.7.8	不可	

(B)

図8



9  
[X]



## (署名生成)

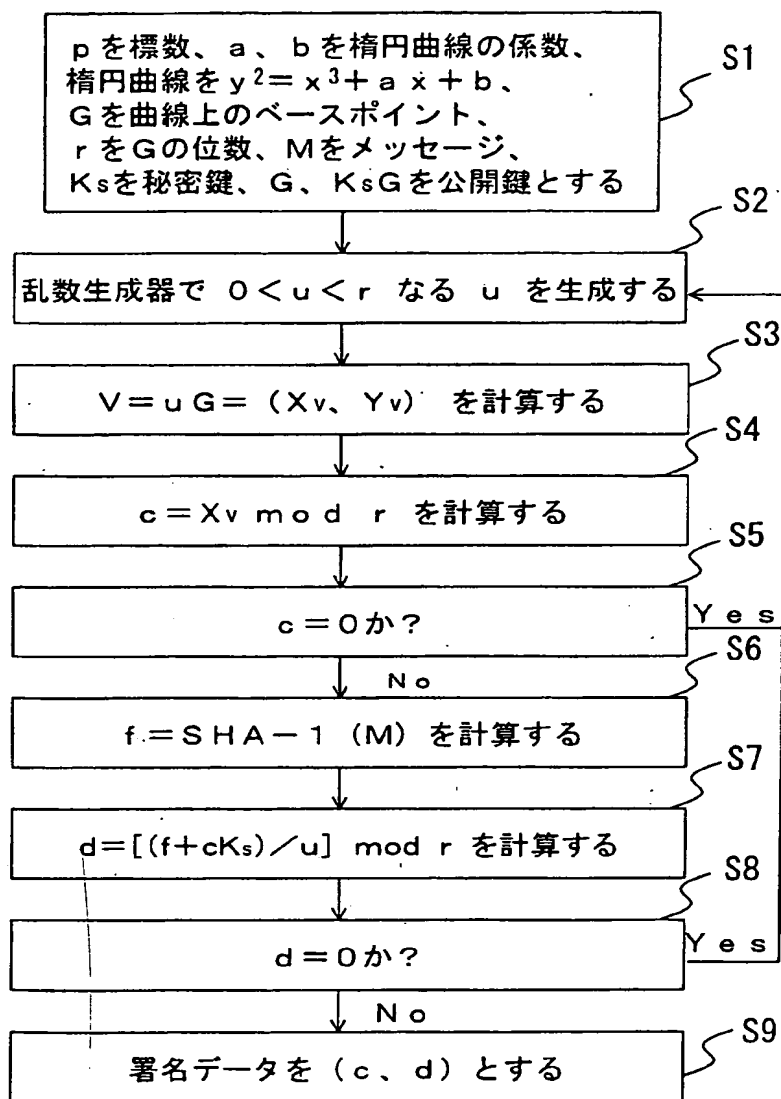


図 10

## (署名検証)

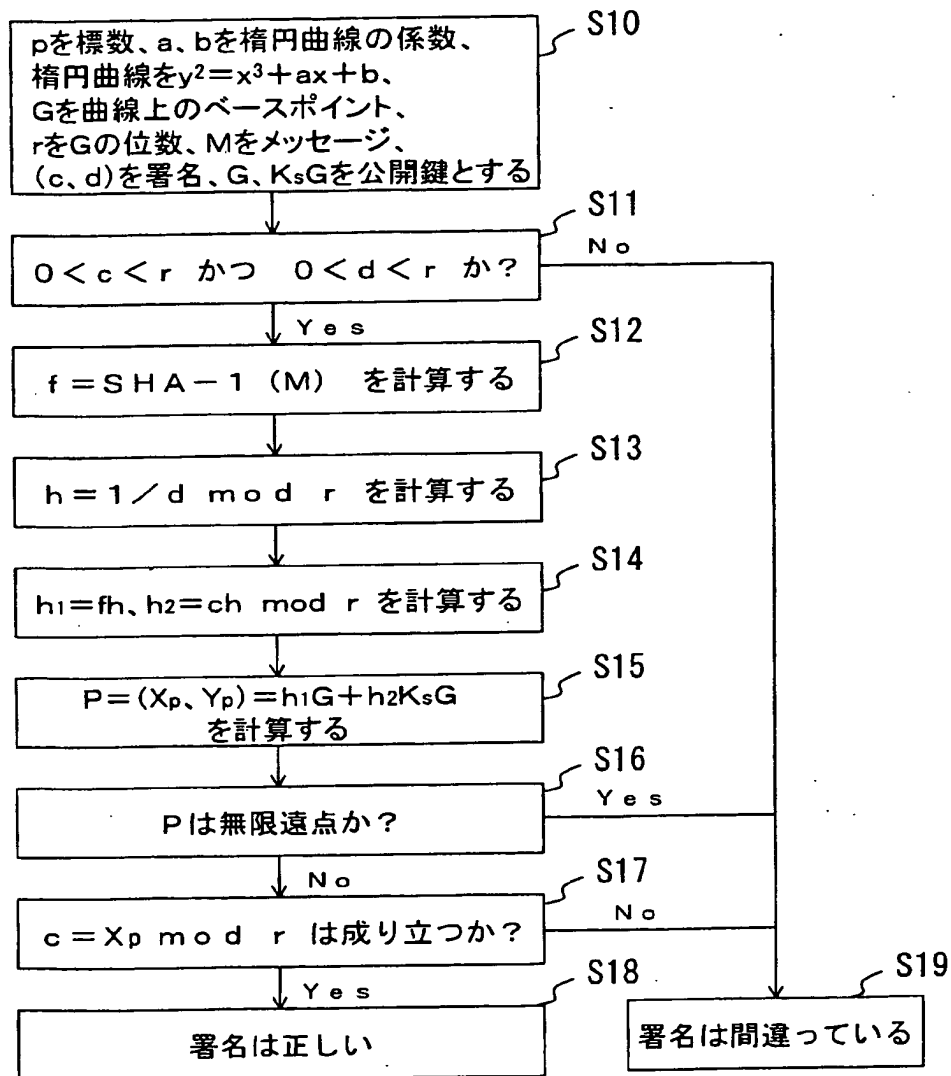


図 1 1

## (暗号化)

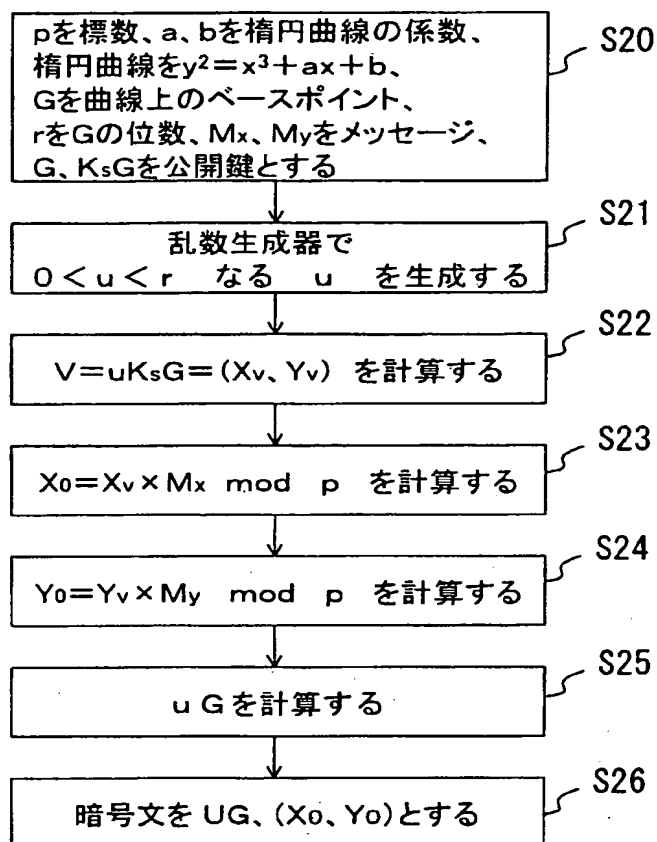


図 1 2

(復号化)

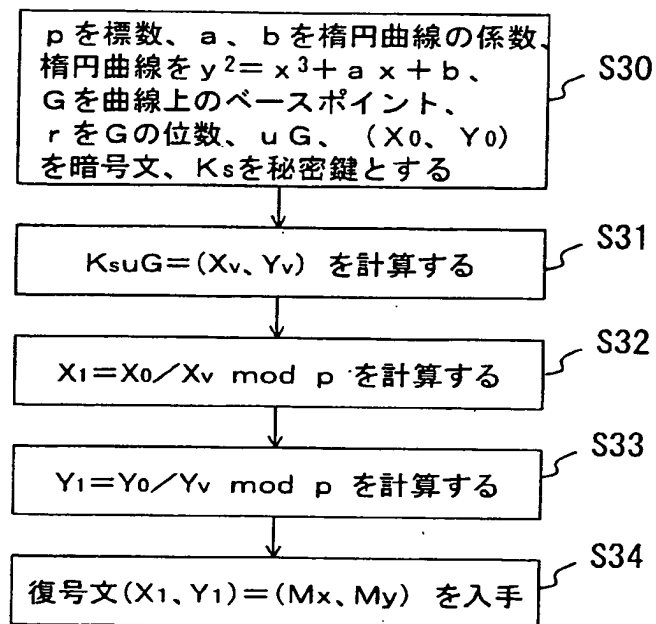
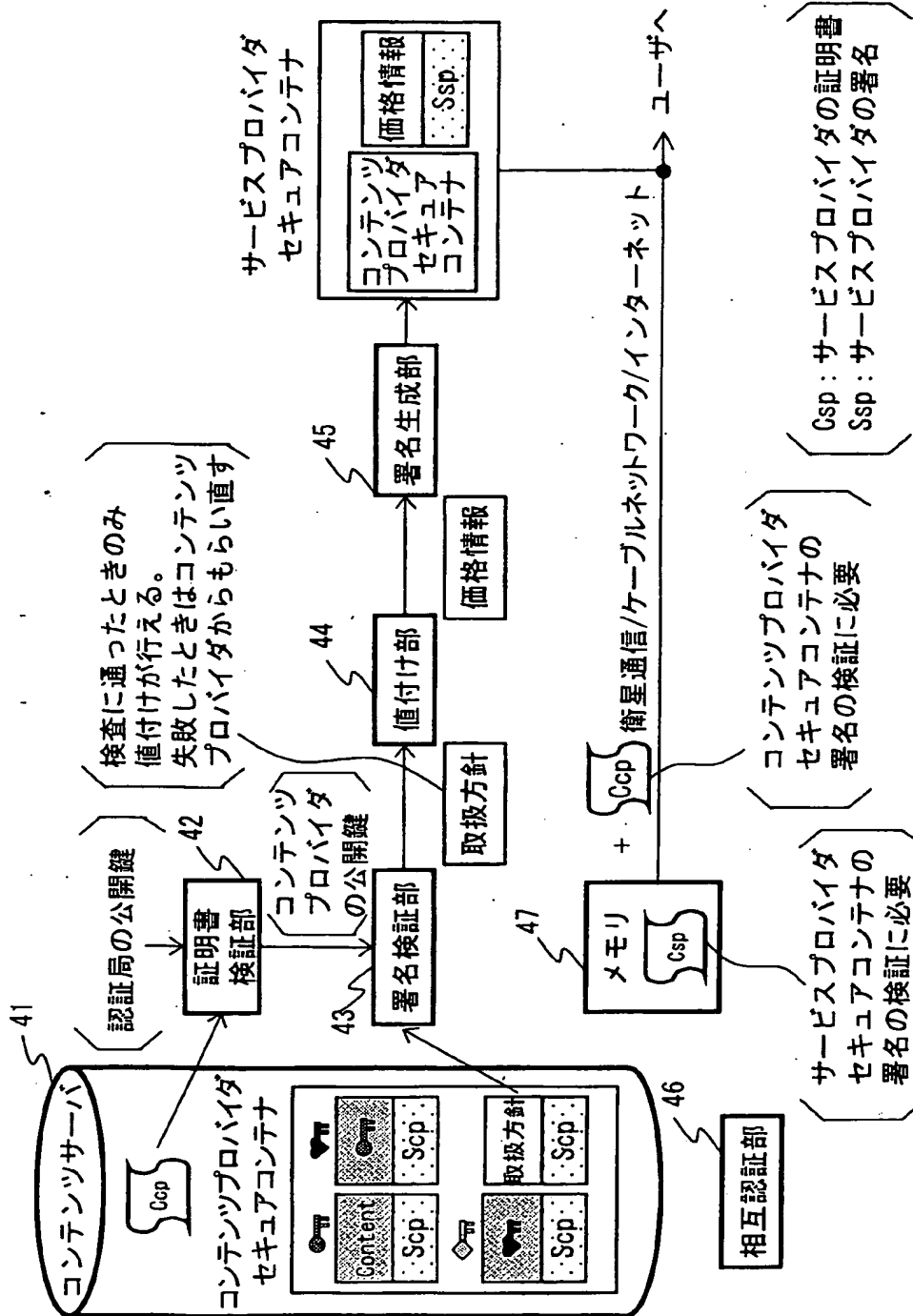


図 13



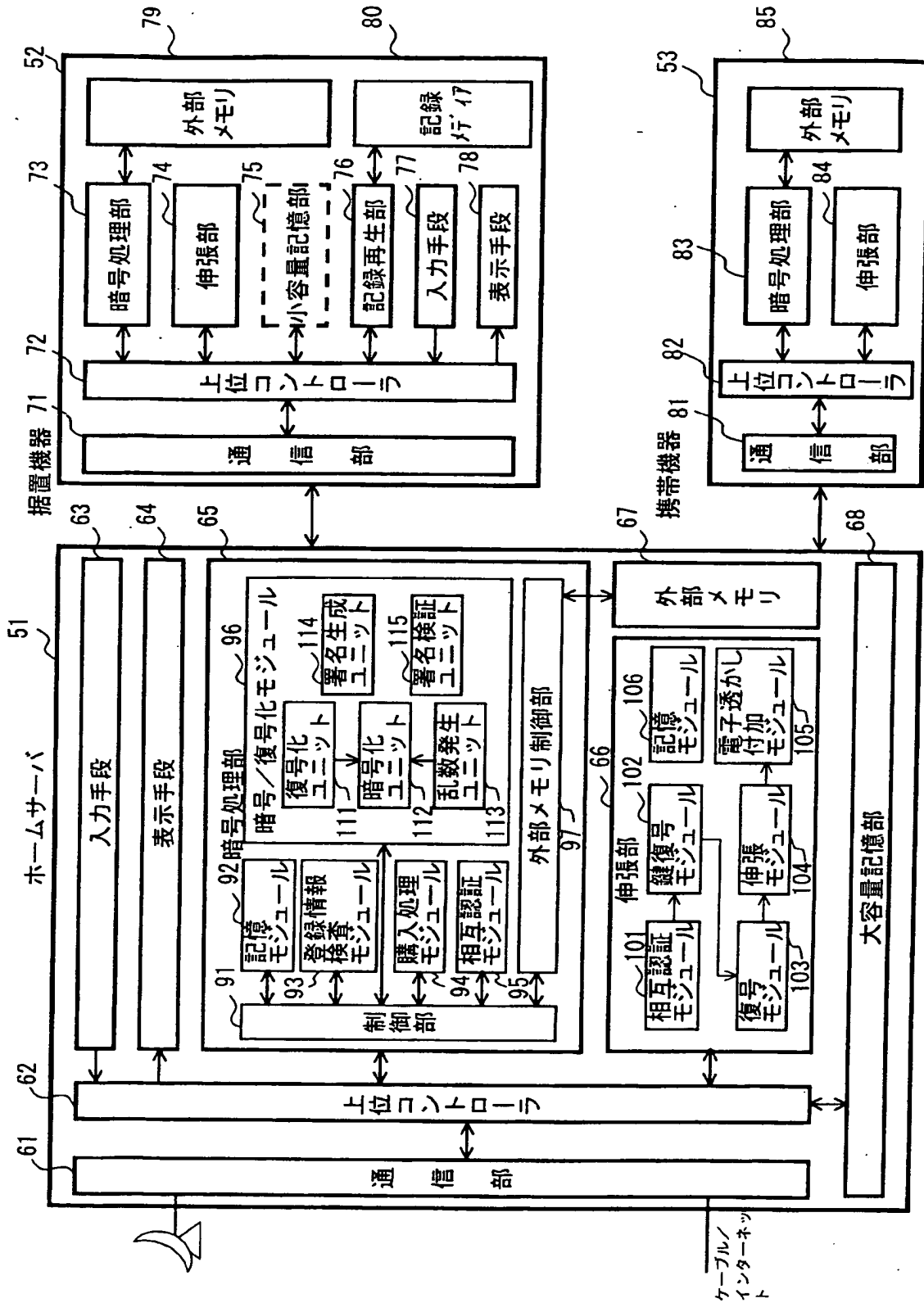


図15

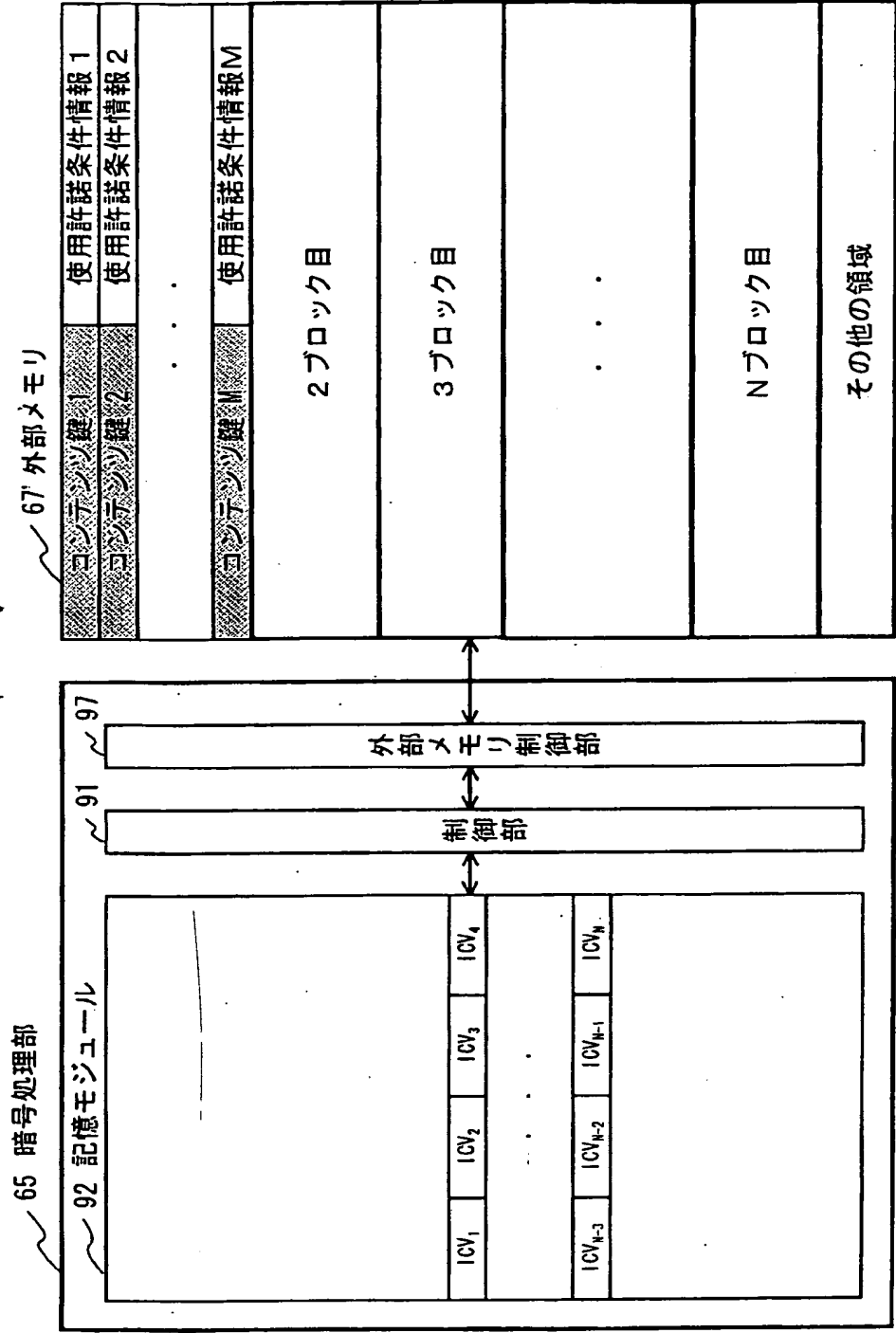


図16

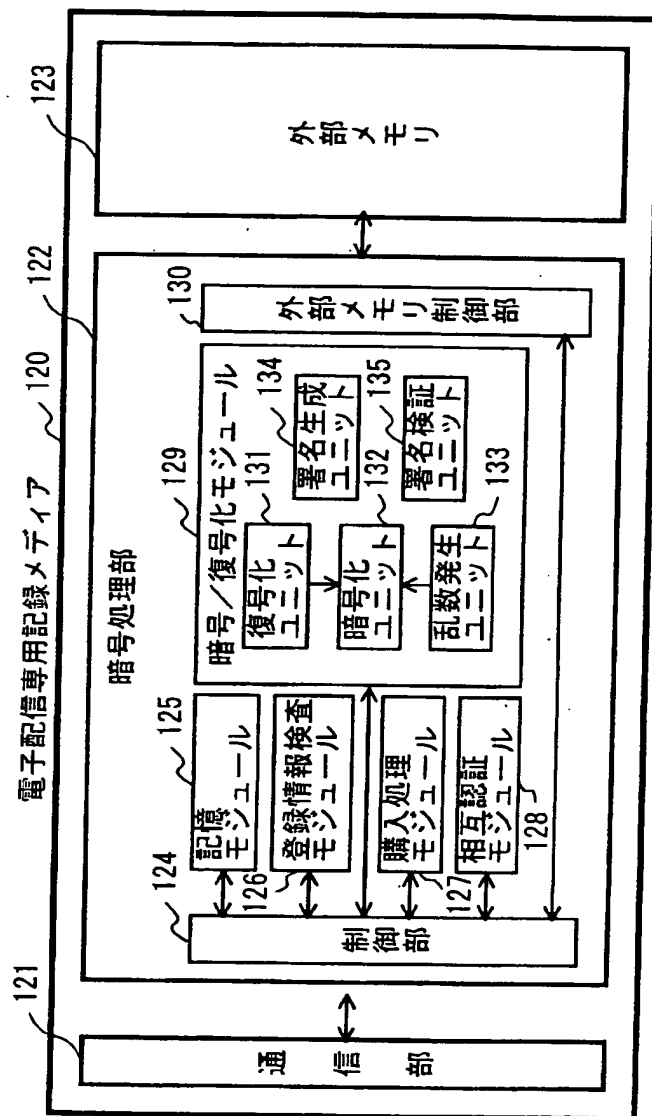


図 17



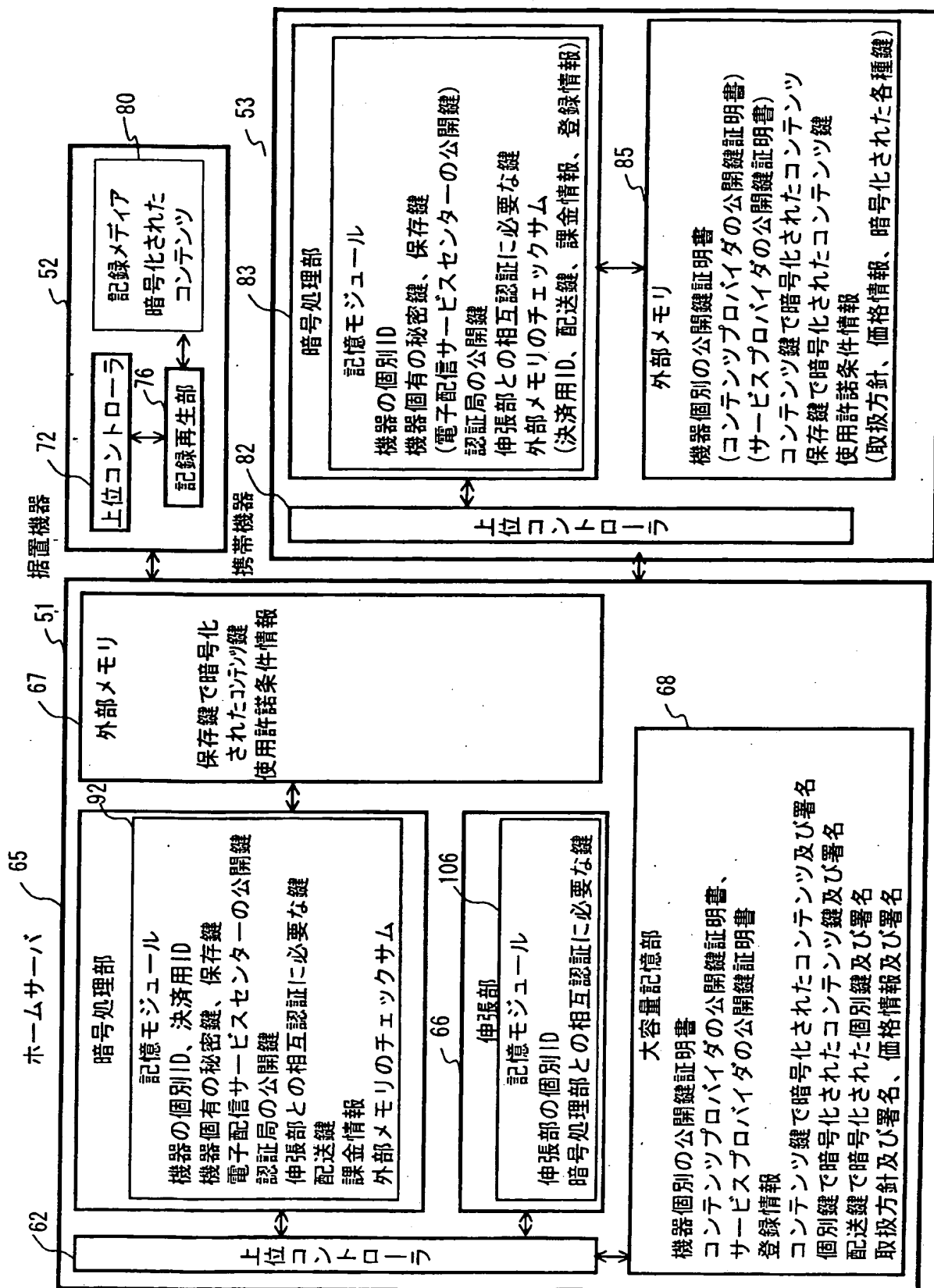


図 18

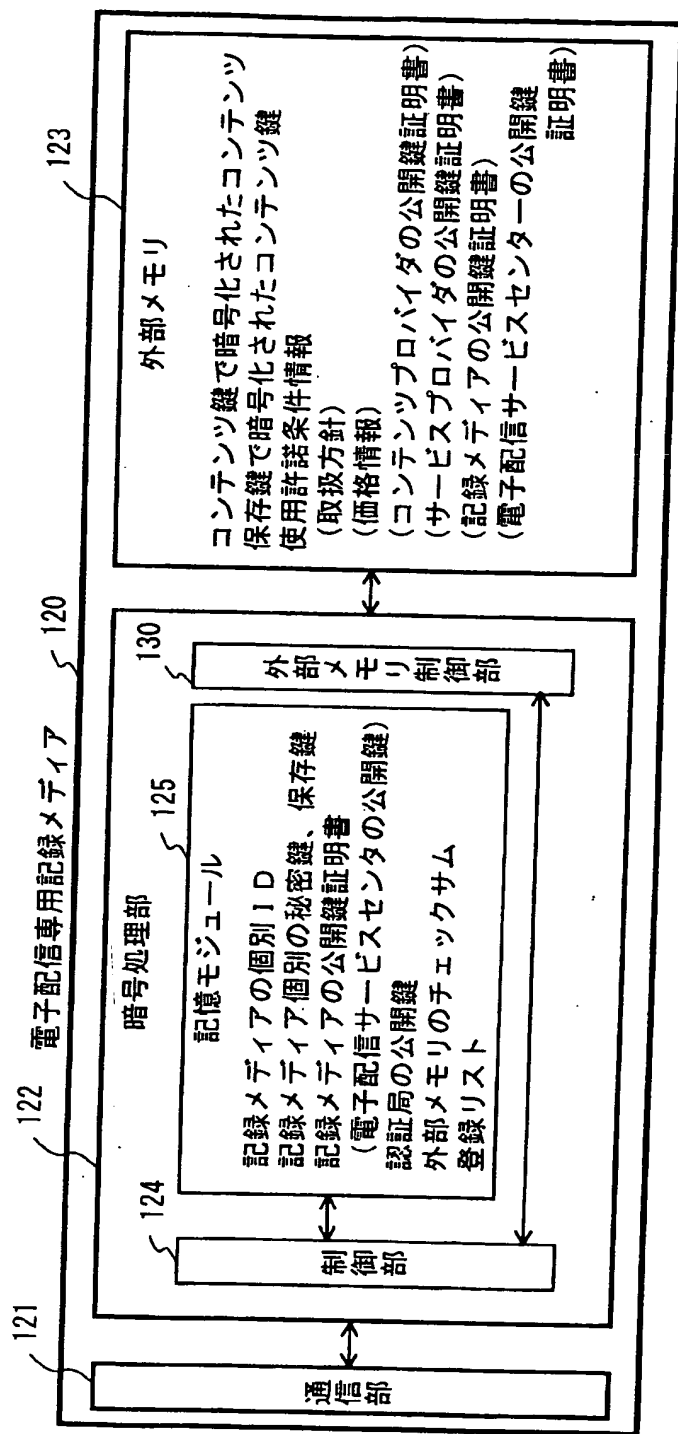


図19

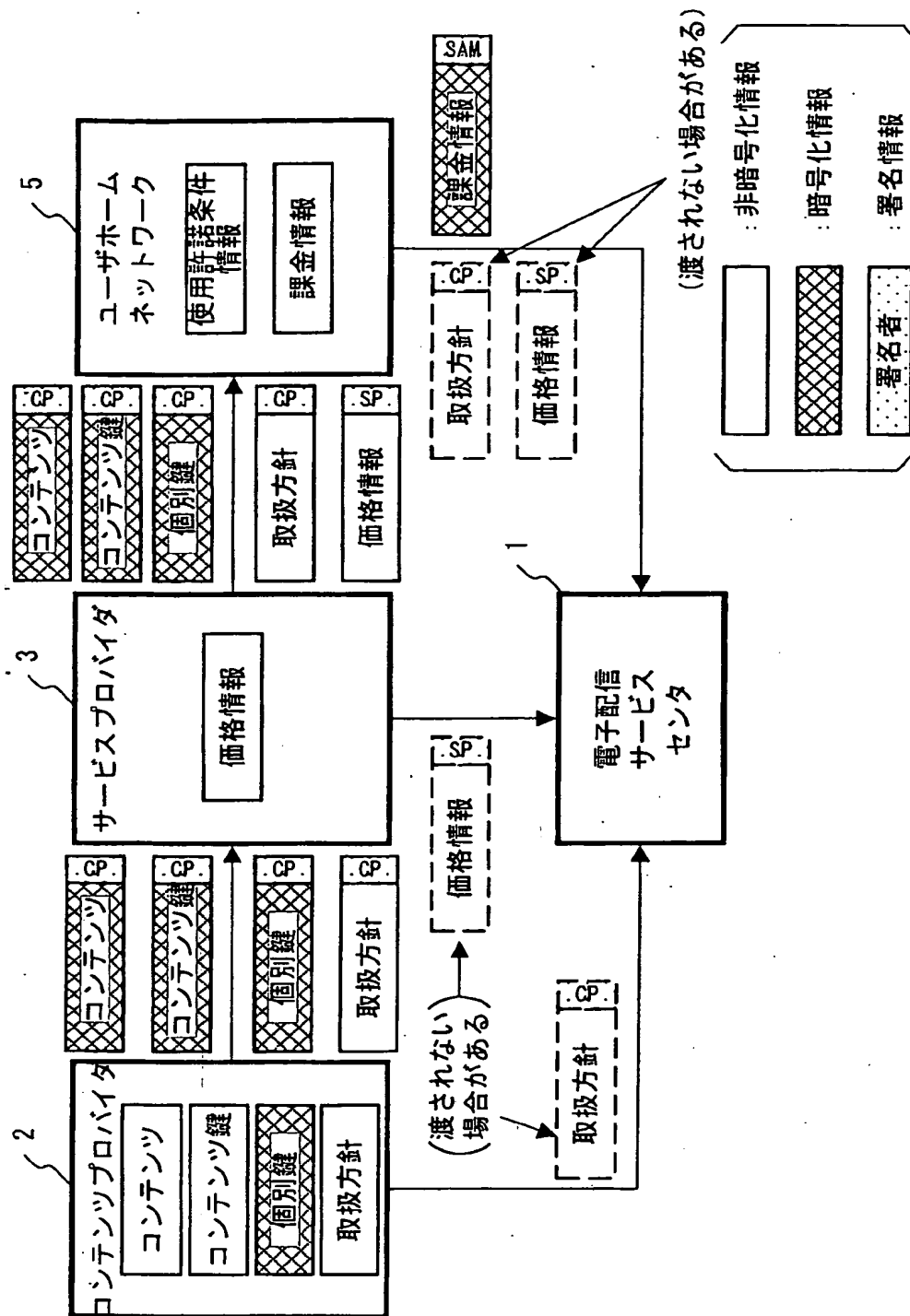


図 20

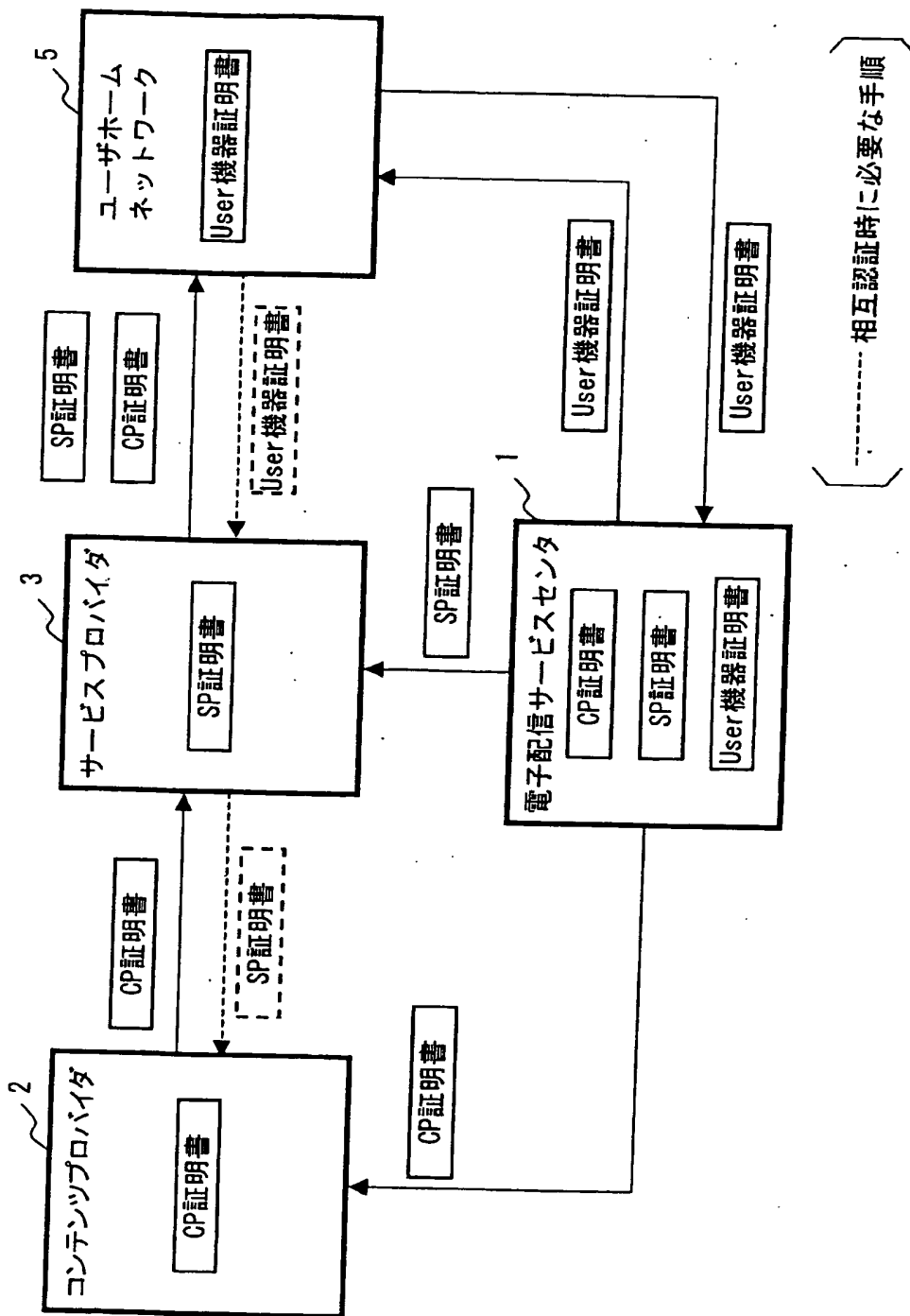


図 21

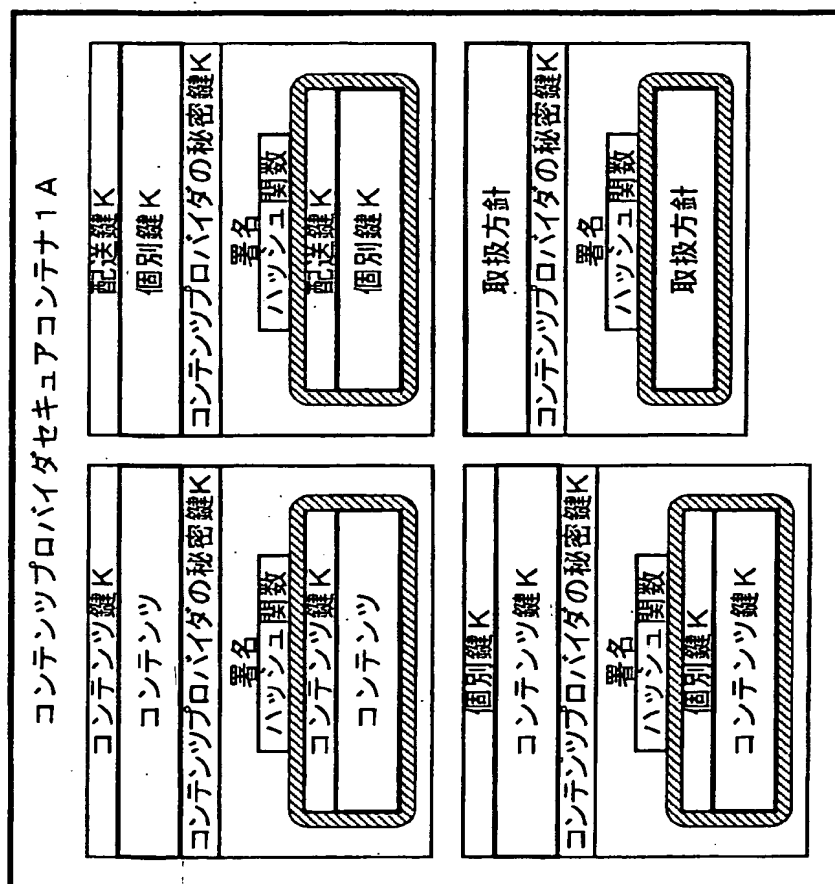


図 22

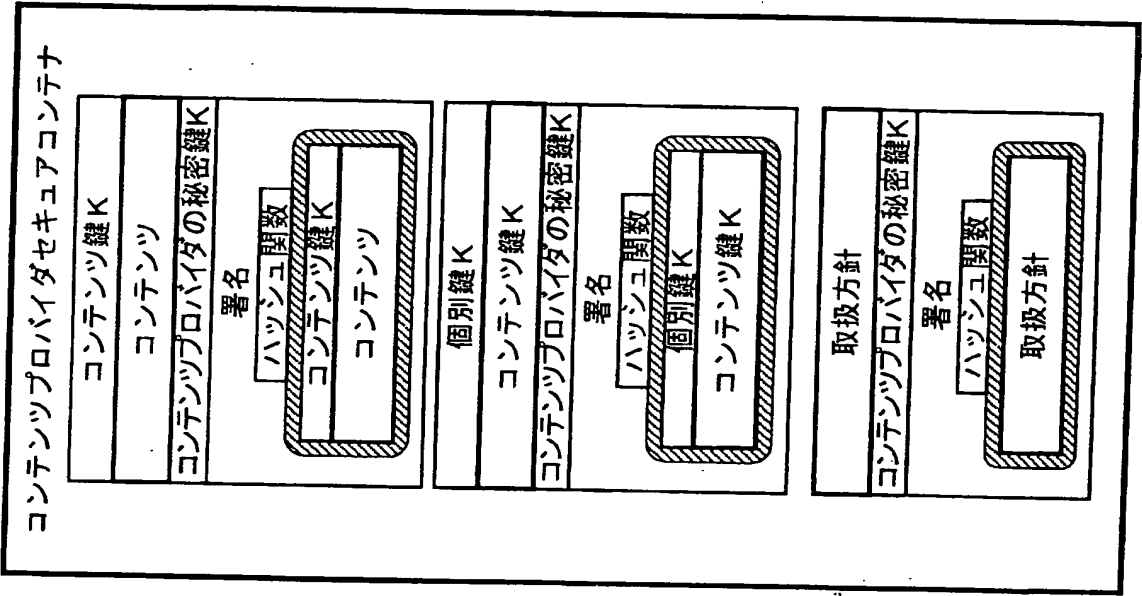


図 23

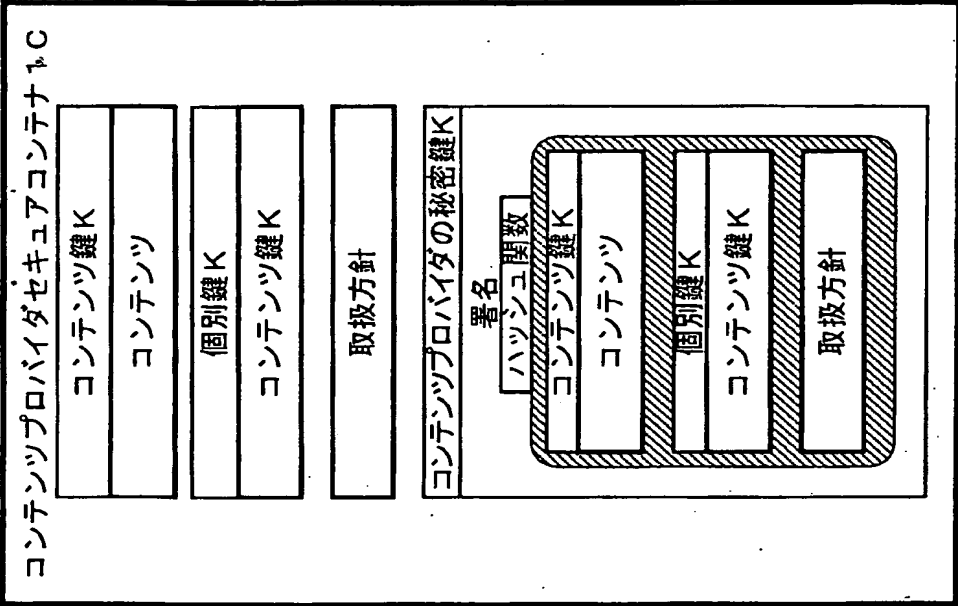


図 2 4

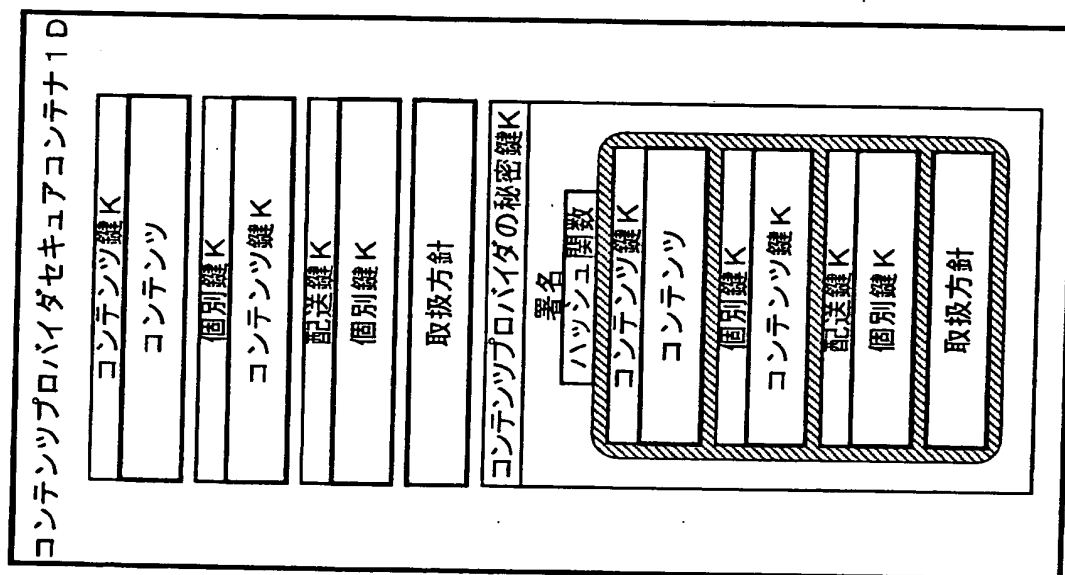


図 25



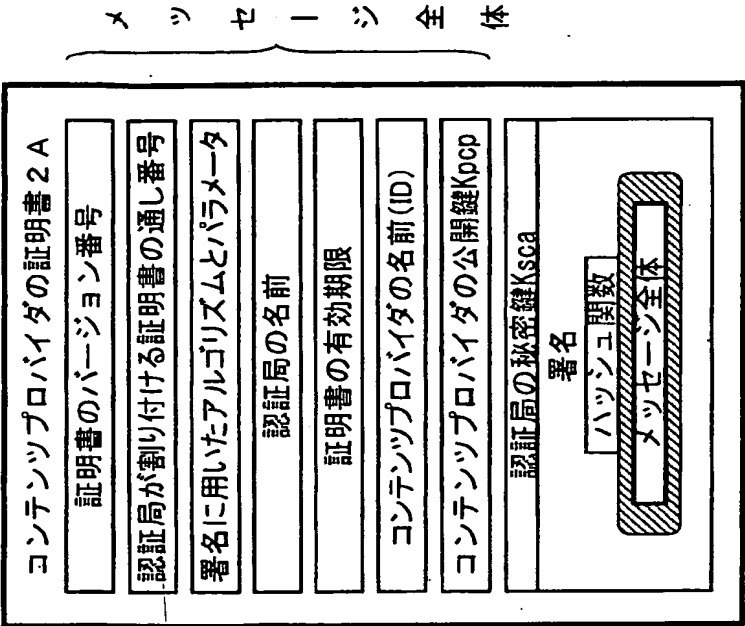
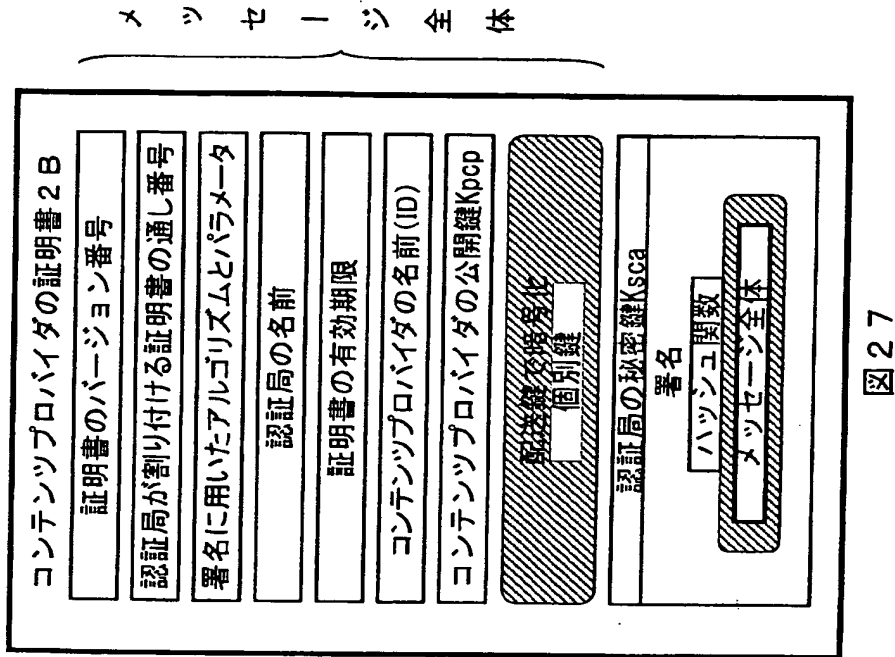


図 2 6



メ ッ セ ー ジ 全 体

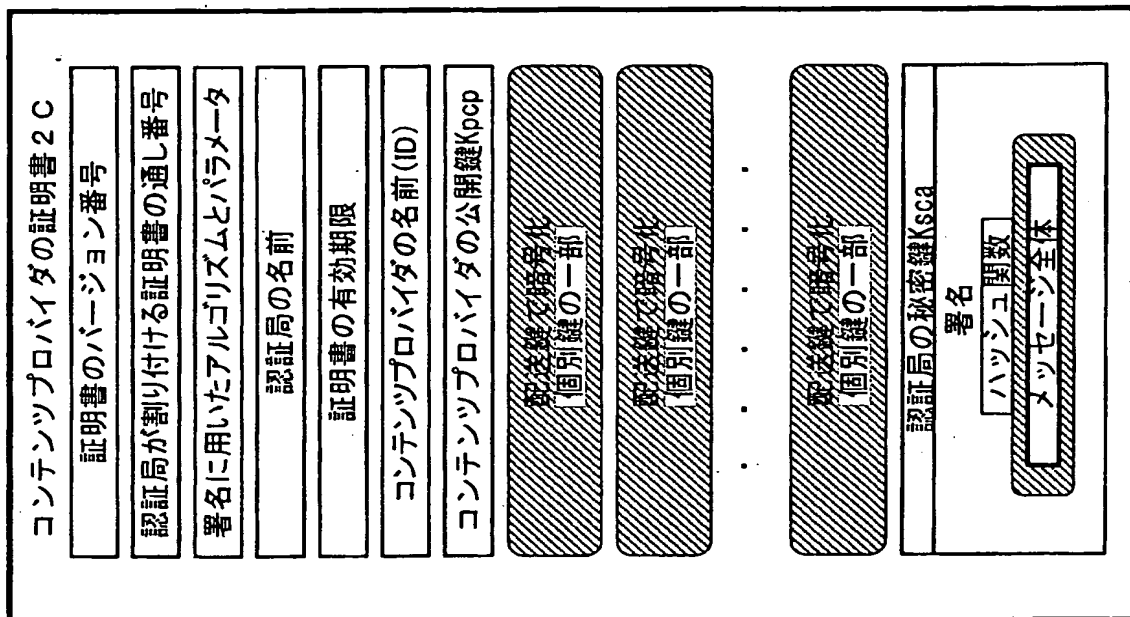


図 28

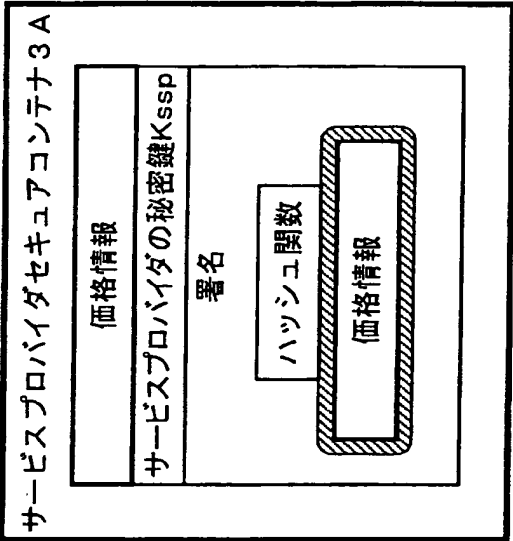


図 29

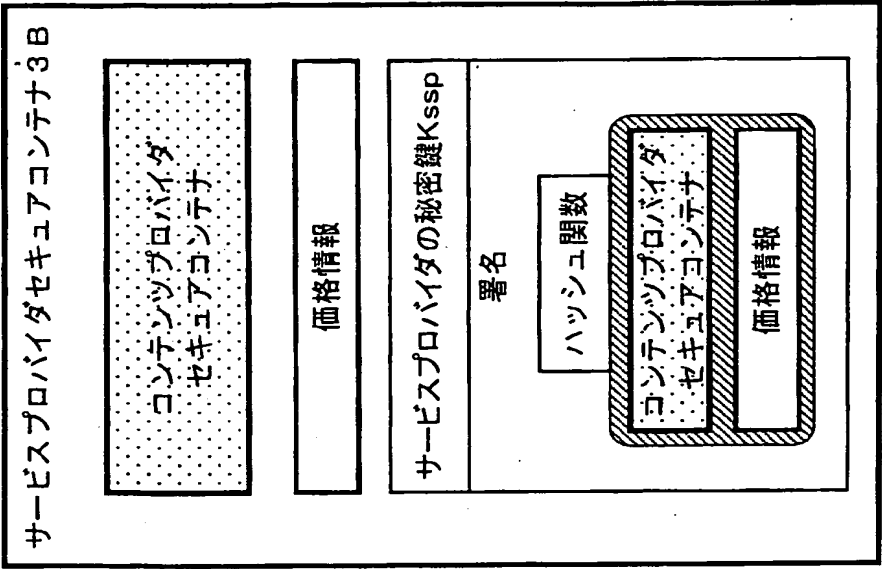


図 30

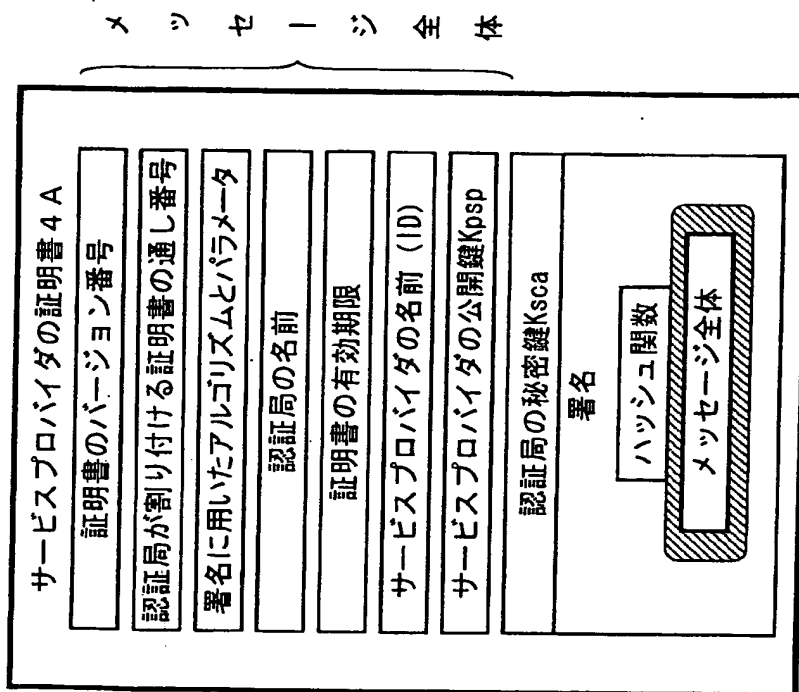


図 3 1

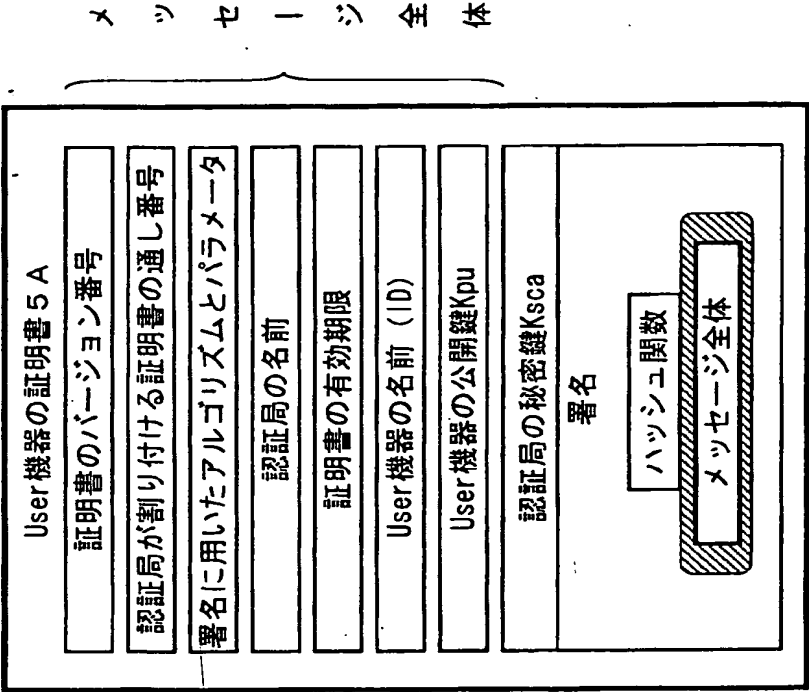


図 3 2

データの種別	
取扱方針の種類（シングル）	
取扱方針の有効期限	
コンテンツの I D	
コンテンツプロバイダの I D	
取扱方針の I D	
取扱方針のバージョン	
地域コード	
使用可能機器条件	
使用可能User条件	
サービスプロバイダの I D	
世代管理情報	
ルールの数	
ルールアドレス情報	
ル ー ル 1	ルール番号（Rule#）
	利用権内容番号（Type）
	パラメータ
	最低販売価格
	コンテンツプロバイダの利益額
	コンテンツプロバイダの利益率
	データサイズ
	送信情報
⋮	⋮
ル ー ル N	ルール番号（Rule#）
	利用権内容番号（Type）
	パラメータ
	最低販売価格
	コンテンツプロバイダの利益額
	コンテンツプロバイダの利益率
	データサイズ
	送信情報
（署名の検証の有無）	
公開鍵証明書	
署名	

図 3 3



データの種別	
取扱方針の種類 (アルバム)	
取扱方針の有効期限	
アルバムのID	
取扱方針のバージョン	
コンテンツプロバイダのID	
取扱方針のID	
地域コード	
使用可能機器条件	
使用可能User条件	
サービスプロバイダのID	
シングルコンテンツの取扱方針の数	
シングルコンテンツの取扱方針のアドレス情報	
シングル	取扱方針1
	⋮
	取扱方針N
世代管理情報	
ルール数	
ルールのアドレス情報	
ルール1	ルール番号 (Rule#)
	利用権内容番号 (Type)
	パラメータ
	最低販売価格
	コンテンツプロバイダの利益額
	コンテンツプロバイダの利益率
	データサイズ
	送信情報
⋮	⋮
ルールN	ルール番号 (Rule#)
	利用権内容番号 (Type)
	パラメータ
	最低販売価格
	コンテンツプロバイダの利益額
	コンテンツプロバイダの利益率
	データサイズ
	送信情報
(署名の検出の有無)	
公開鍵証明書	
署名	

図 3 4

データの種別	
取扱方針の種類（シングル）	
取扱方針の有効期限	
コンテンツのID	
コンテンツプロバイダのID	
取扱方針のID	
取扱方針のバージョン	
地域コード	
使用可能機器条件	
使用可能User条件	
サービスプロバイダのID	
世代管理情報	
ルール数	
ルールのアドレス情報	
ルール 1	ルール番号（Rule#）
	利用権内容番号（Type）
	パラメータ
	最低販売価格
	データサイズ
	送信情報
...	...
ルール N	ルール番号（Rule#）
	利用権内容番号（Type）
	パラメータ
	最低販売価格
	データサイズ
	送信情報
（署名の検出の有無）	
公開鍵証明書	
署名	

図 3 5

データの種別	
取扱方針の種類（アルバム）	
取扱方針の有効期限	
アルバムのID	
取扱方針のバージョン	
コンテンツプロバイダのID	
取扱方針のID	
地域コード	
使用可能機器条件	
使用可能User条件	
サービスプロバイダのID	
シングルコンテンツの取扱方針の数	
シングルコンテンツの取扱方針のアドレス情報	
シングル	取扱方針1
	⋮
	取扱方針N
世代管理情報	
ルールの数	
ルールのアドレス情報	
ルール1	ルール番号 (Rule#)
	利用権内容番号 (Type)
	パラメータ
	最低販売価格
	データサイズ
	送信情報
⋮	⋮
ルールN	ルール番号 (Rule#)
	利用権内容番号 (Type)
	パラメータ
	最低販売価格
	データサイズ
	送信情報
(署名の検出の有無)	
公開鍵証明書	
署名	

図 3 6

データの種別	
価格情報の種類 (シングル)	
価格情報の有効期限	
コンテンツの I D	
サービスプロバイダの I D	
価格情報の I D	
価格情報のバージョン	
地域コード	
使用可能機器条件	
使用可能User条件	
コンテンツプロバイダの I D	
取扱方針の I D	
ルールの数	
ルールアドレス情報	
ル ー ル 1	ルール番号 (Rule#)
	サービスプロバイダの利益額
	サービスプロバイダの利益率
	価格
	データサイズ
	送信情報
⋮	⋮
ル ー ル N	ルール番号 (Rule#)
	サービスプロバイダの利益額
	サービスプロバイダの利益率
	価格
	データサイズ
	送信情報
(署名の検出の有無)	
公開鍵証明書	
署名	

図.3 7

データの種別	
価格情報の種類 (アルバム)	
価格情報の有効期限	
アルバムのID	
サービスプロバイダのID	
価格情報のID	
価格情報のバージョン	
地域コード	
使用可能機器条件	
使用可能User条件	
コンテンツプロバイダのID	
取扱方針のID	
シングルコンテンツの価格情報の数	
シングルコンテンツの価格情報のアドレス情報	
シングル	価格情報1
	⋮
	価格情報N
ルールの数	
ルールアドレス情報	
ルール1	ルール番号 (Rule#)
	サービスプロバイダの利益額
	サービスプロバイダの利益率
	価格
	データサイズ
	送信情報
⋮	⋮
ルールN	ルール番号 (Rule#)
	サービスプロバイダの利益額
	サービスプロバイダの利益率
	価格
	データサイズ
	送信情報
(署名の検出の有無)	
公開鍵証明書	
署名	

図 3 8

データの種別	
価格情報の種類（シングル）	
価格情報の有効期限	
コンテンツのID	
サービスプロバイダのID	
価格情報のID	
価格情報のバージョン	
地域コード	
使用可能機器条件	
使用可能User条件	
コンテンツプロバイダのID	
取扱方針のID	
ルールの数	
ルールアドレス情報	
ル ー ル 1	ルール番号（Rule#）
	価格
	データサイズ
	送信情報
⋮	⋮
ル ー ル N	ルール番号（Rule#）
	価格
	データサイズ
	送信情報
（署名の検出の有無）	
公開鍵証明書	
署名	

図 3 9

データの種別	
価格情報の種類 (アルバム)	
価格情報の有効期限	
アルバムのID	
サービスプロバイダのID	
価格情報のID	
価格情報のバージョン	
地域コード	
使用可能機器条件	
使用可能User条件	
コンテンツプロバイダのID	
取扱方針のID	
シングルコンテンツの価格情報の数	
シングルコンテンツの価格情報のアドレス情報	
シングル	価格情報1
	⋮
	価格情報N
ルール数	
ルールのアドレス情報	
ルール1	ルール番号 (Rule#)
	価格
	データサイズ
	送信情報
⋮	⋮
ルールN	ルール番号 (Rule#)
	価格
	データサイズ
	送信情報
(署名の検出の有無)	
公開鍵証明書	
署名	

図 40

データの種別
使用許諾条件情報の種類
使用許諾条件情報の有効期限
コンテンツの I D
アルバムの I D
暗号処理部の I D
ユーザの I D
コンテンツプロバイダの I D
取扱方針の I D
取扱方針のバージョン
サービスプロバイダの I D
価格情報の I D
価格情報のバージョン
使用許諾条件情報の I D
再生権（利用権）のルール番号
利用権内容番号
再生残り回数
再生権の有効期限
複製権（利用権）のルール番号
利用権内容番号
複製残り回数
世代管理情報
再生権を保有する暗号処理部の I D

図 4 1



データの種別
暗号処理部の I D
ユーザの I D
コンテンツの I D
コンテンツプロバイダの I D
取扱方針の I D
取扱方針のバージョン
サービスプロバイダの I D
価格情報の I D
価格情報のバージョン
使用許諾条件の I D
ルール番号 (Rule#)
コンテンツプロバイダの利益額／利益率
サービスプロバイダの利益額／利益率
世代管理情報
コンテンツプロバイダの設定した送信情報のデータサイズ
コンテンツプロバイダの設定した送信情報
サービスプロバイダの設定した送信情報のデータサイズ
サービスプロバイダの設定した送信情報
供給元の I D

図 4 2

データの種別
暗号処理部の I D
ユーザの I D
コンテンツの I D
コンテンツプロバイダの I D
取扱方針の I D
取扱方針のバージョン
サービスプロバイダの I D
価格情報の I D
価格情報のバージョン
使用許諾条件の I D
ルール番号 (Rule#)
世代管理情報
コンテンツプロバイダの設定した送信情報のデータサイズ
コンテンツプロバイダの設定した送信情報
サービスプロバイダの設定した送信情報のデータサイズ
サービスプロバイダの設定した送信情報
供給元の I D

図 4 3

利用権内容番号					利用権内容			
					権利	期間制限	回数制限	複製制限
(1)	再生権					なし	なし	—
(2)						あり	なし	—
(3)						あり	なし	—
(4)						なし	あり	—
(5)	複製権					なし	なし	なし
(6)						なし	あり	なし
(7)						なし	なし	SCMS
(8)						なし	あり	
(9) ~ (15)					予備			
(16)	権利内容変更権						—	
(17)	再購入権						—	
(18)	追加購入権						—	
(19)	管理移動権						—	

図 4 4

A	再生権の有効期限
B	再生権の有効期限
C	再生権の有効期限 日数及び時間
D	再生権の有効期限 再生回数
E	複製権の有効期限
F	複製権の有効期限 複製回数
G	複製権の有効期限
H	複製権の有効期限 複製回数
I	権利内容変更権の有効期限 旧ルール番号 新ルール番号
J	再購入権の有効期限 旧ルール番号 新ルール番号 最大再配信世代情報
K	追加購入権の有効期限 最小保有コンテンツ数 最大保有コンテンツ数
L	管理移動権の有効期限
M	コンテンツ購入権の有効期限 旧コンテンツのID 旧ルール番号 新ルール番号

図 4 5

データの種別
コンテンツの種類 (シングル)
コンテンツの有効期限
コンテンツのカテゴリ
コンテンツのID
コンテンツプロバイダのID
コンテンツの暗号方式
暗号化したコンテンツのデータ長
暗号化したコンテンツ
公開鍵証明書
署名

図 4 6

データの種別	
コンテンツの種類 (アルバム)	
コンテンツの有効期限	
アルバムの I D	
コンテンツプロバイダの I D	
シングルコンテンツの数	
シングルコンテンツのアドレス情報	
シングル	コンテンツ 1
	⋮
	コンテンツ N
公開鍵証明書	
署名	

図 4 7

データの種別
鍵データの種類 (シングル)
鍵の有効期限
コンテンツのID
コンテンツプロバイダのID
鍵のバージョン
コンテンツ鍵の暗号方式
暗号化したコンテンツ鍵
個別鍵の暗号方式
暗号化した個別鍵
公開鍵証明書
署名

図 4 8

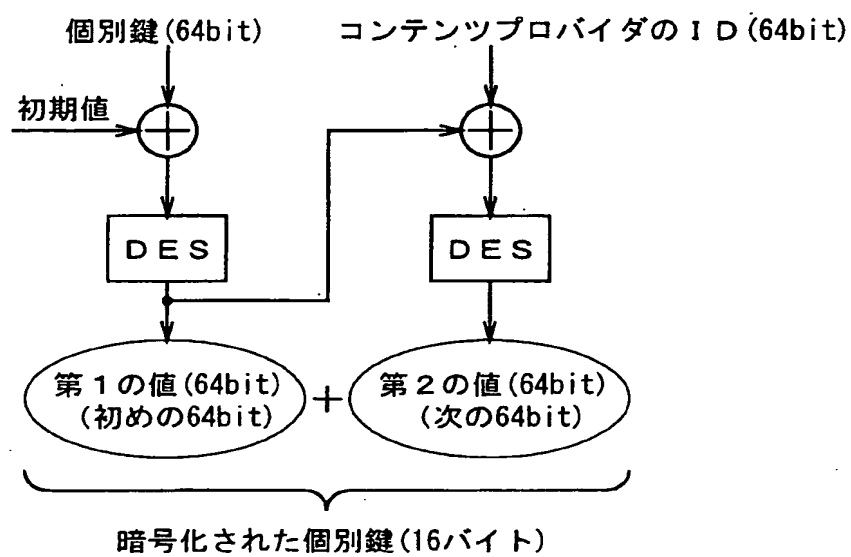


図 4 9



データの種別	
鍵データの種類（アルバム）	
鍵の有効期限	
アルバムのID	
コンテンツプロバイダID	
鍵のバージョン	
シングルコンテンツ用の鍵データの数	
シングルコンテンツ用の鍵データのアドレス情報	
シングル	鍵データ 1
	⋮
	鍵データ N
公開鍵証明書	
署名	

図 5 0

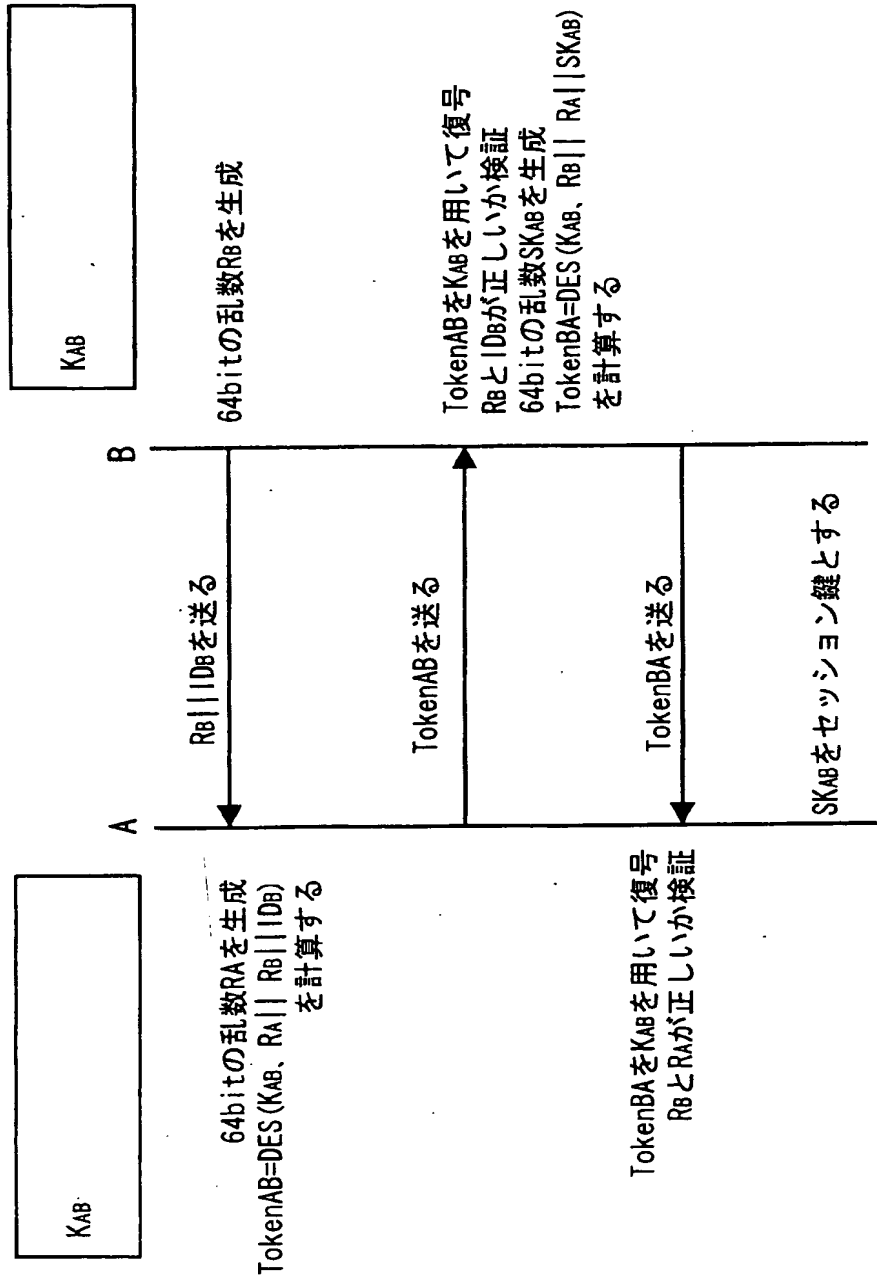


図 5 1

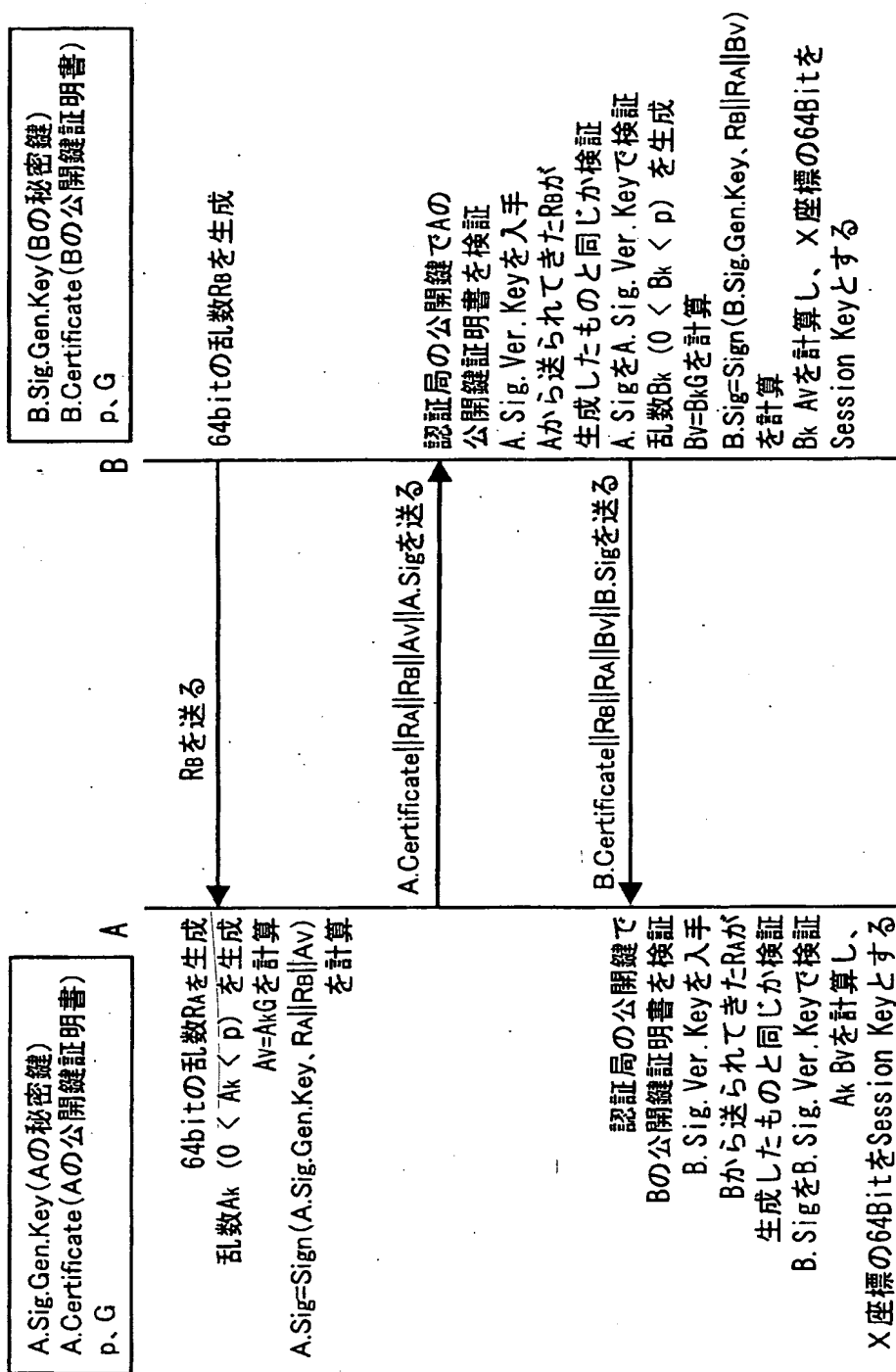


図 5 2

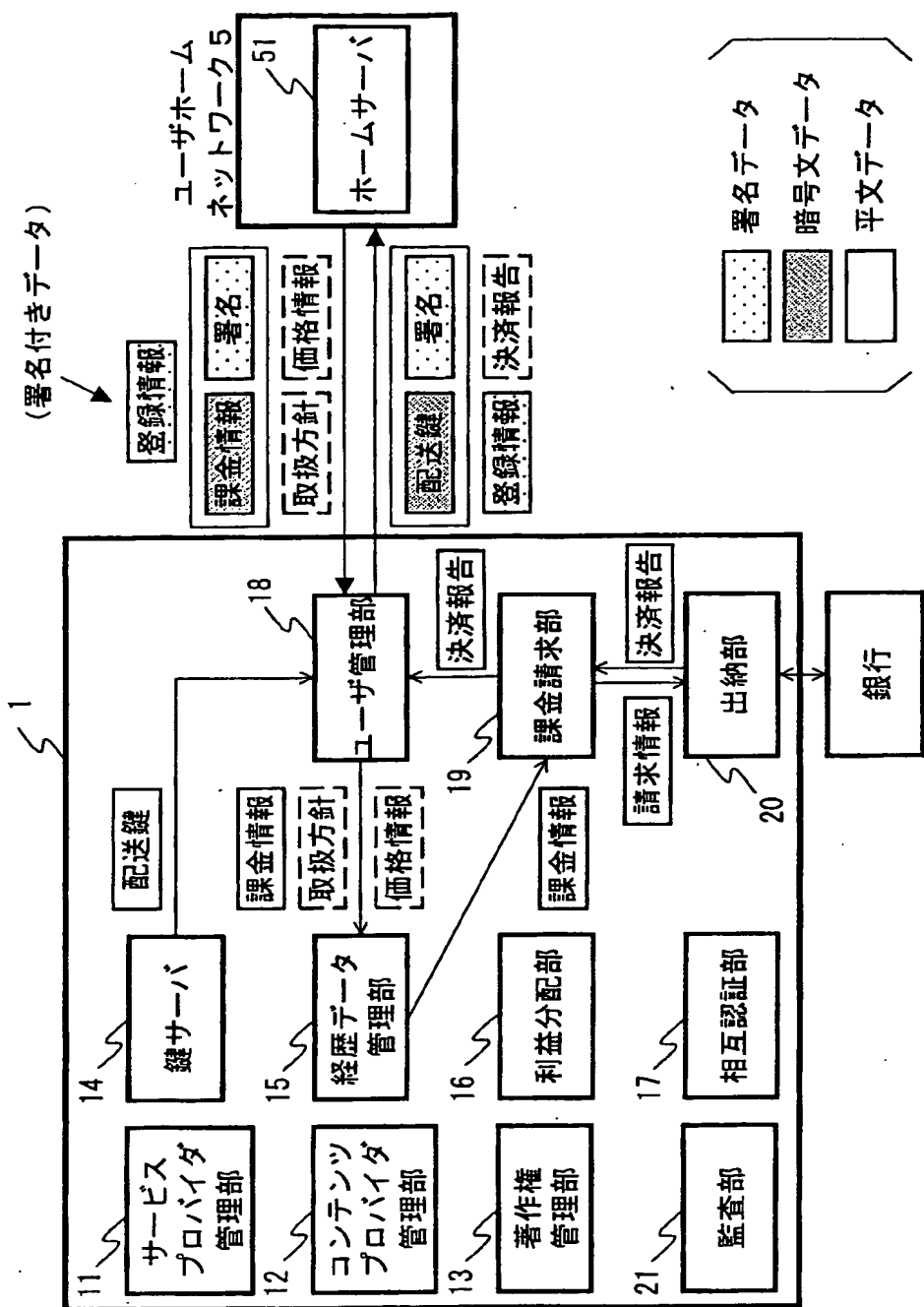


図 53

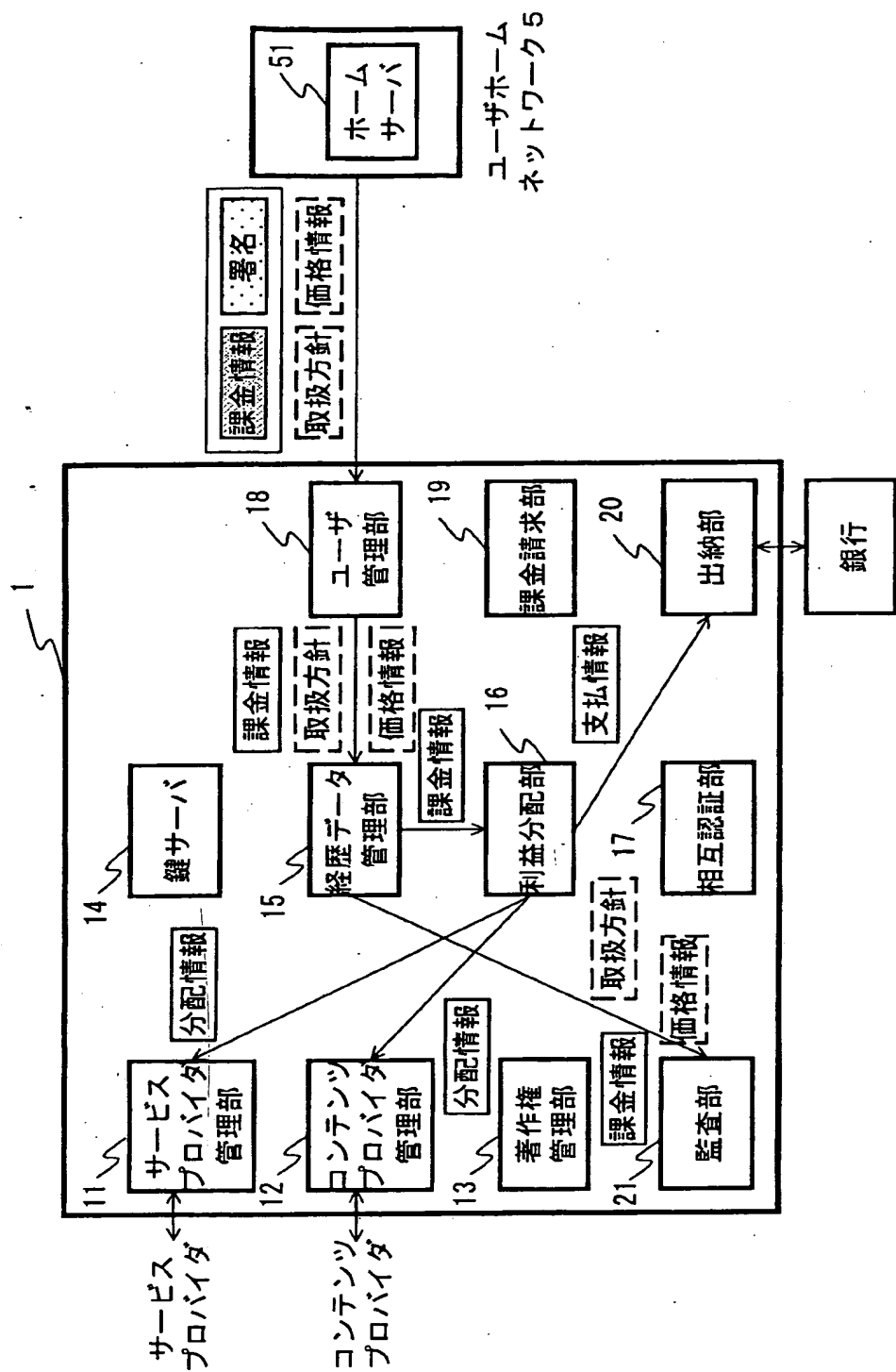


図 54

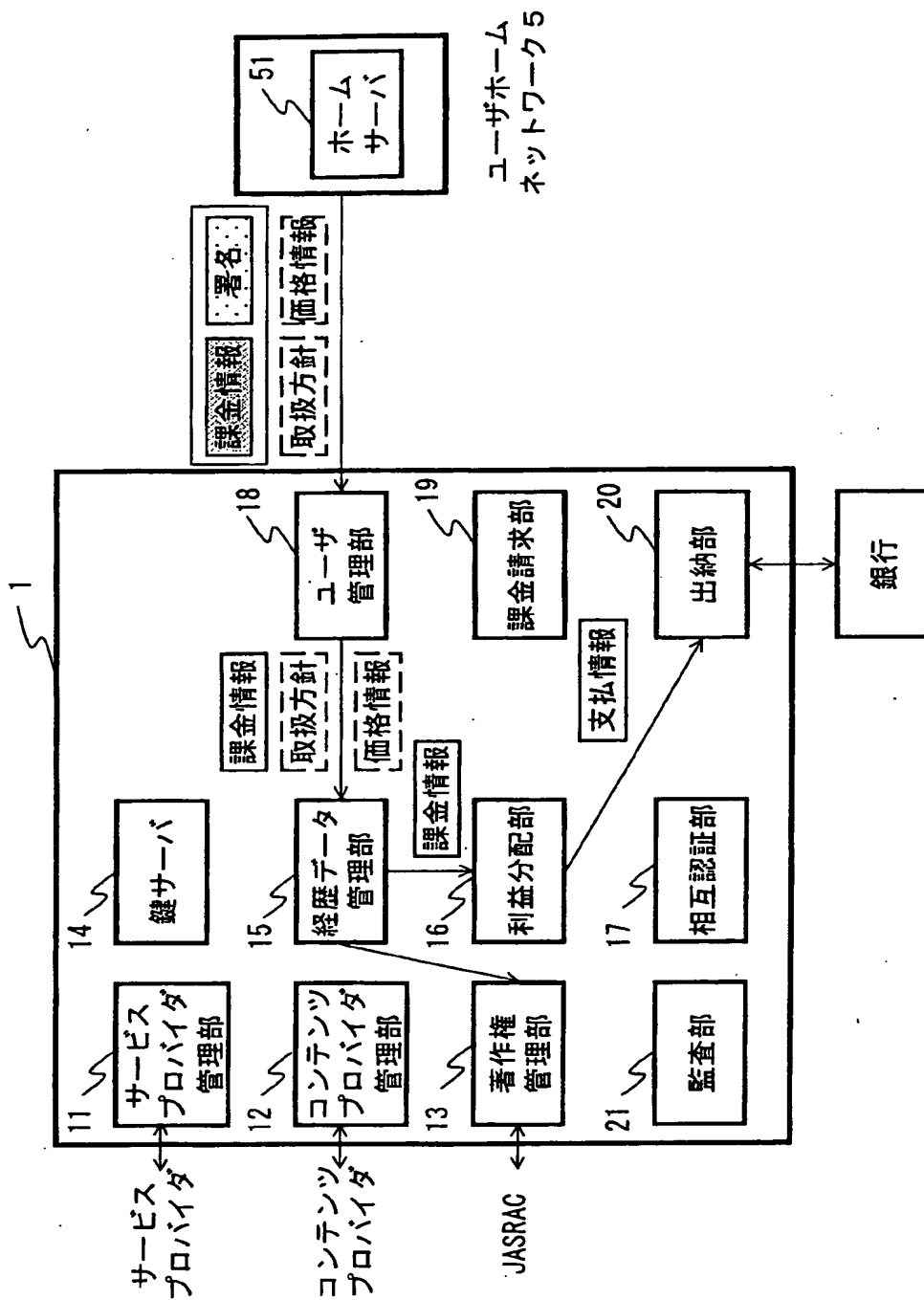


図 55

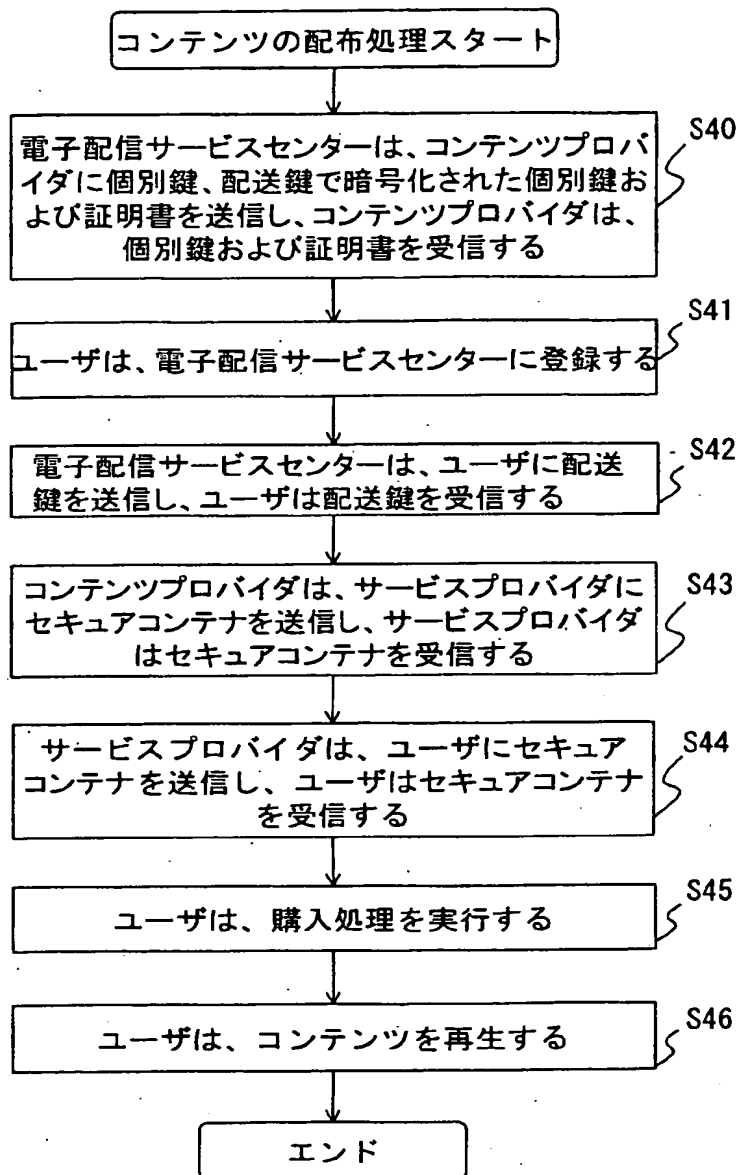


図 5 6

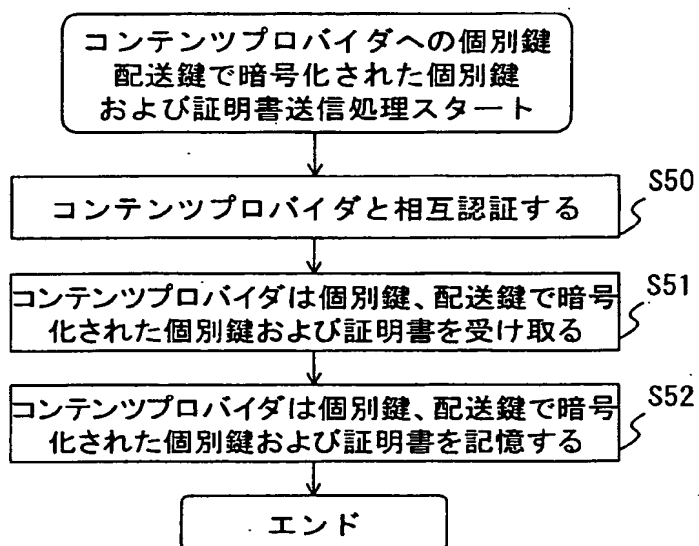


図 5 7



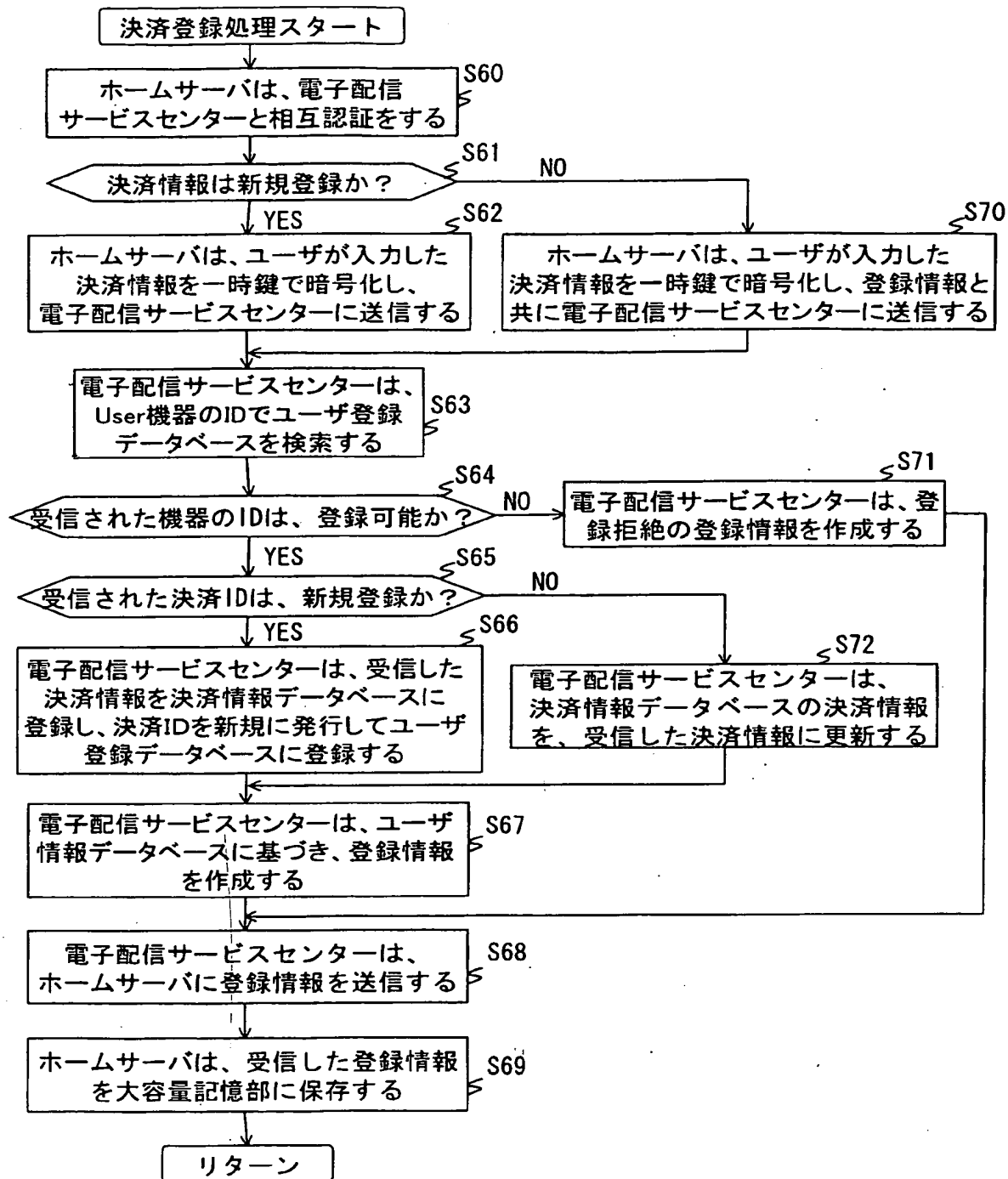


図 5 8

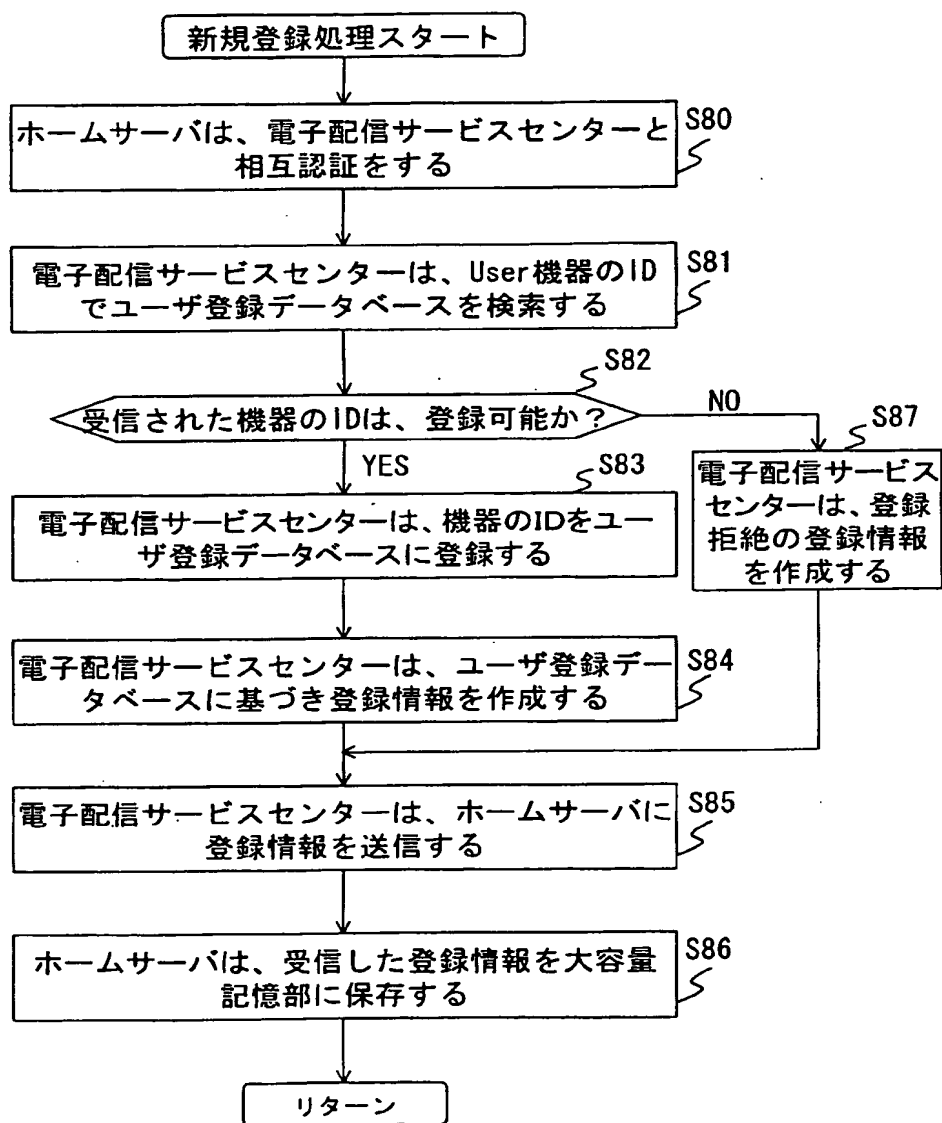


図 5 9

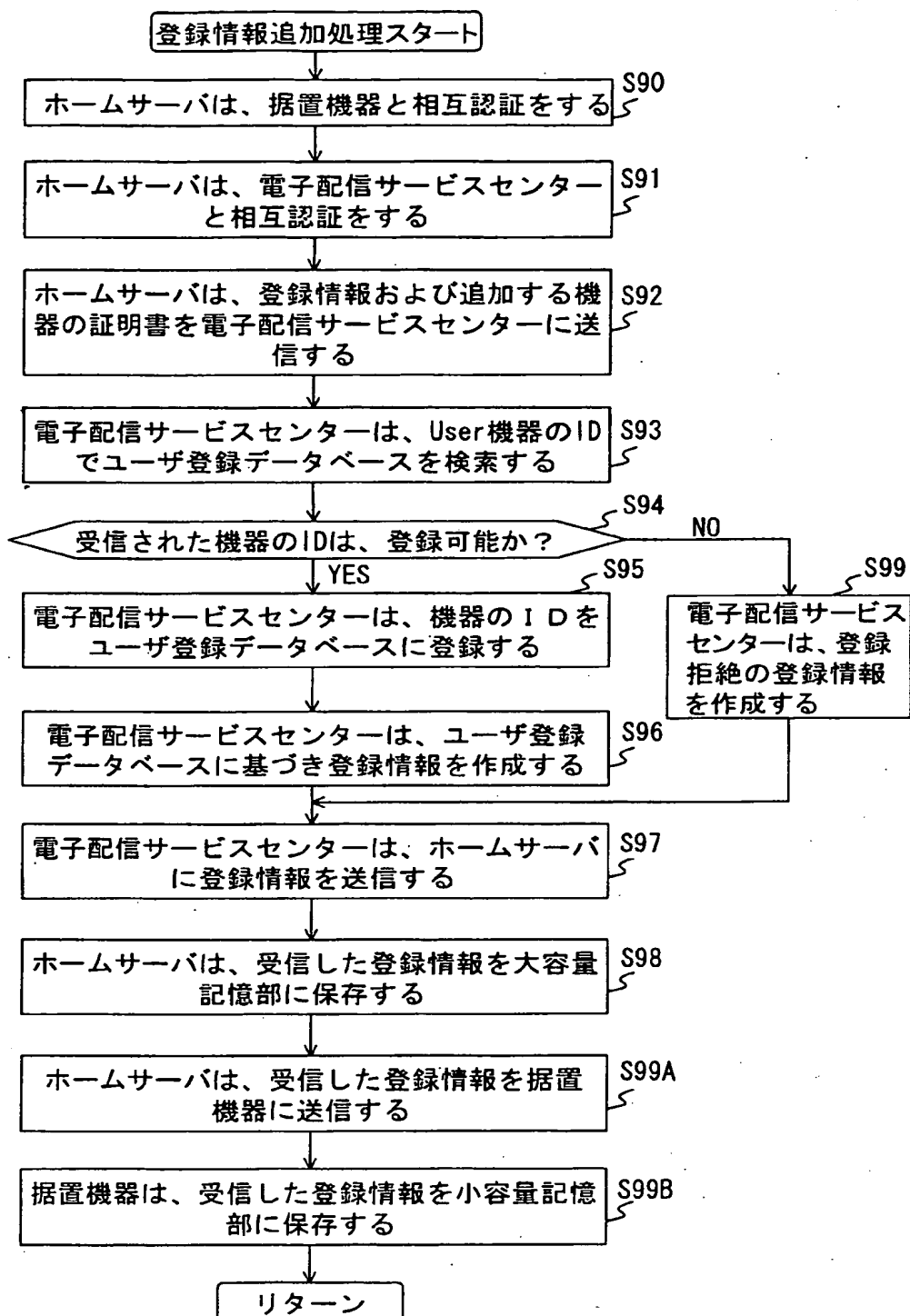


図 6 0

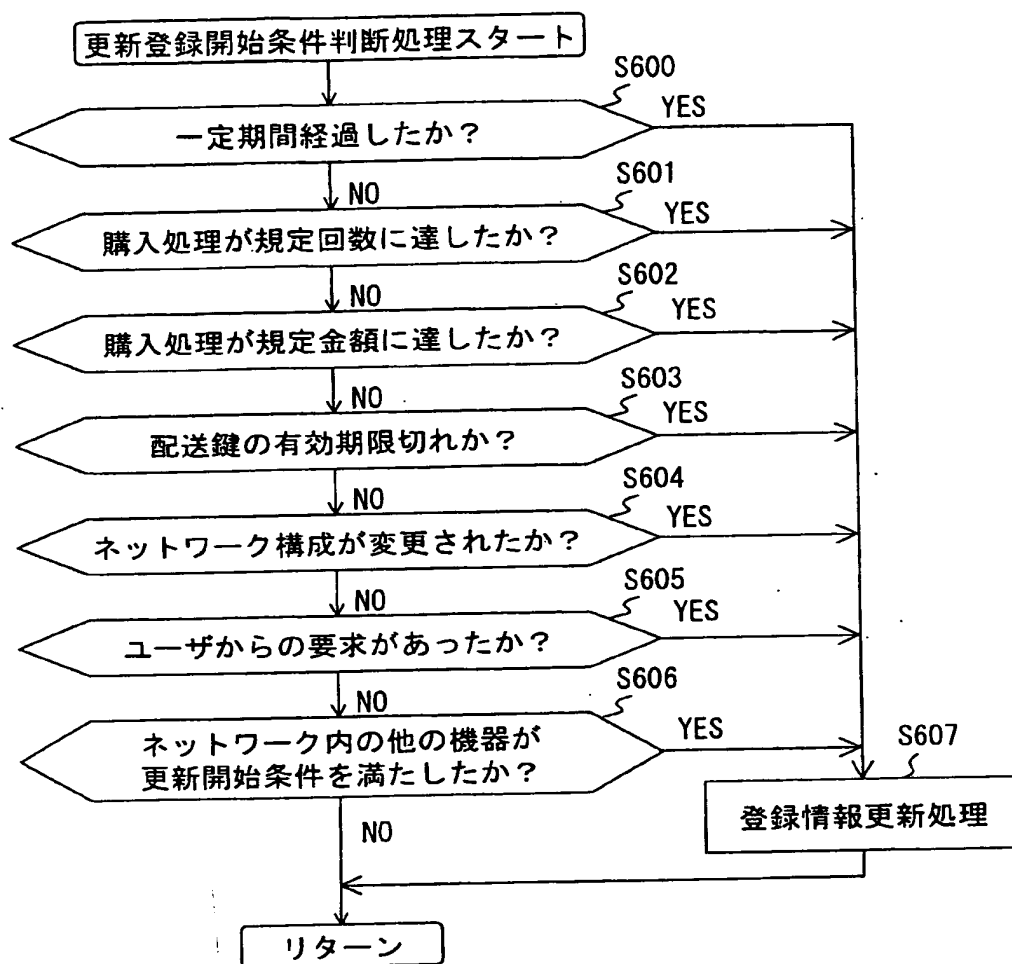


図 6 1

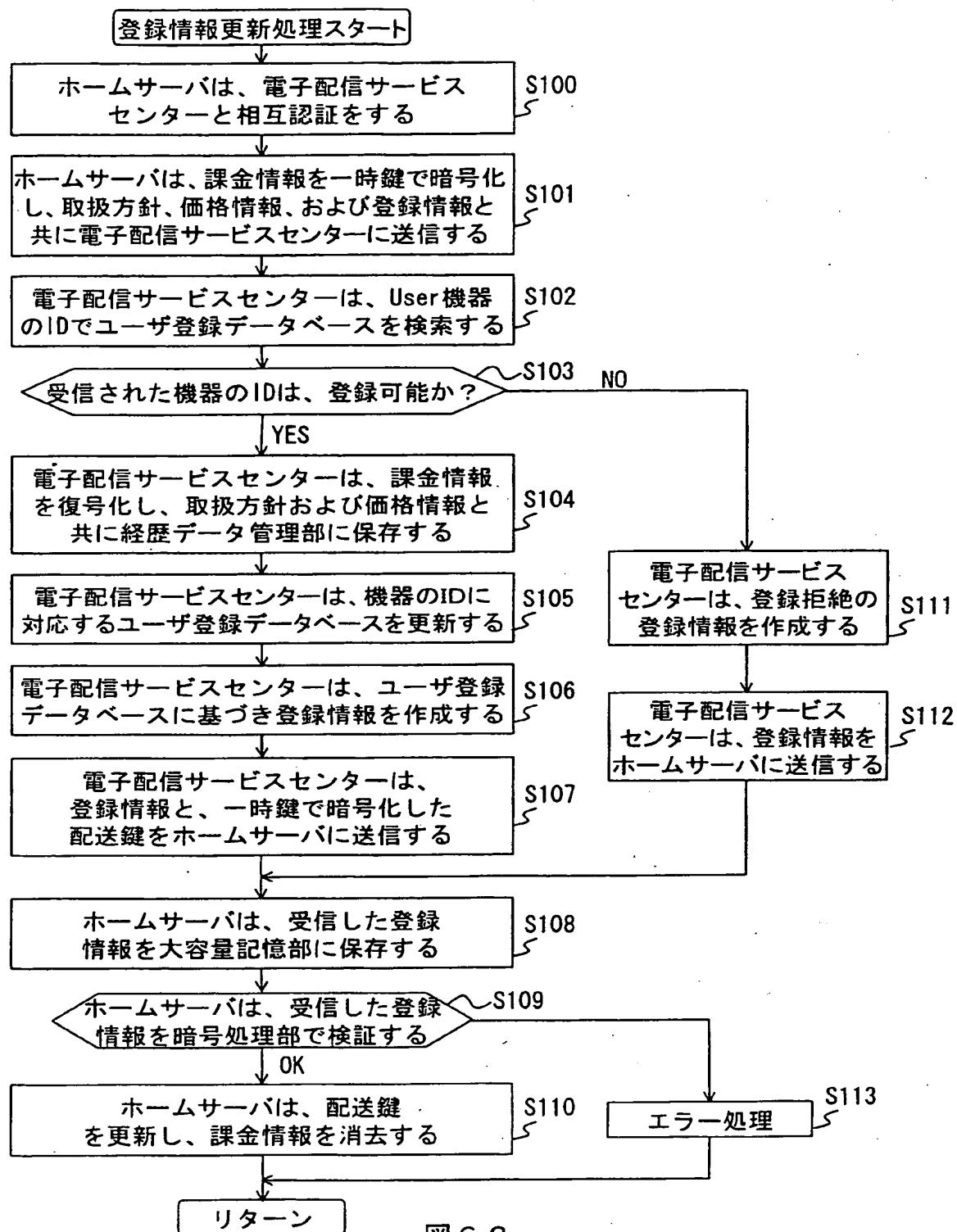


図 6 2

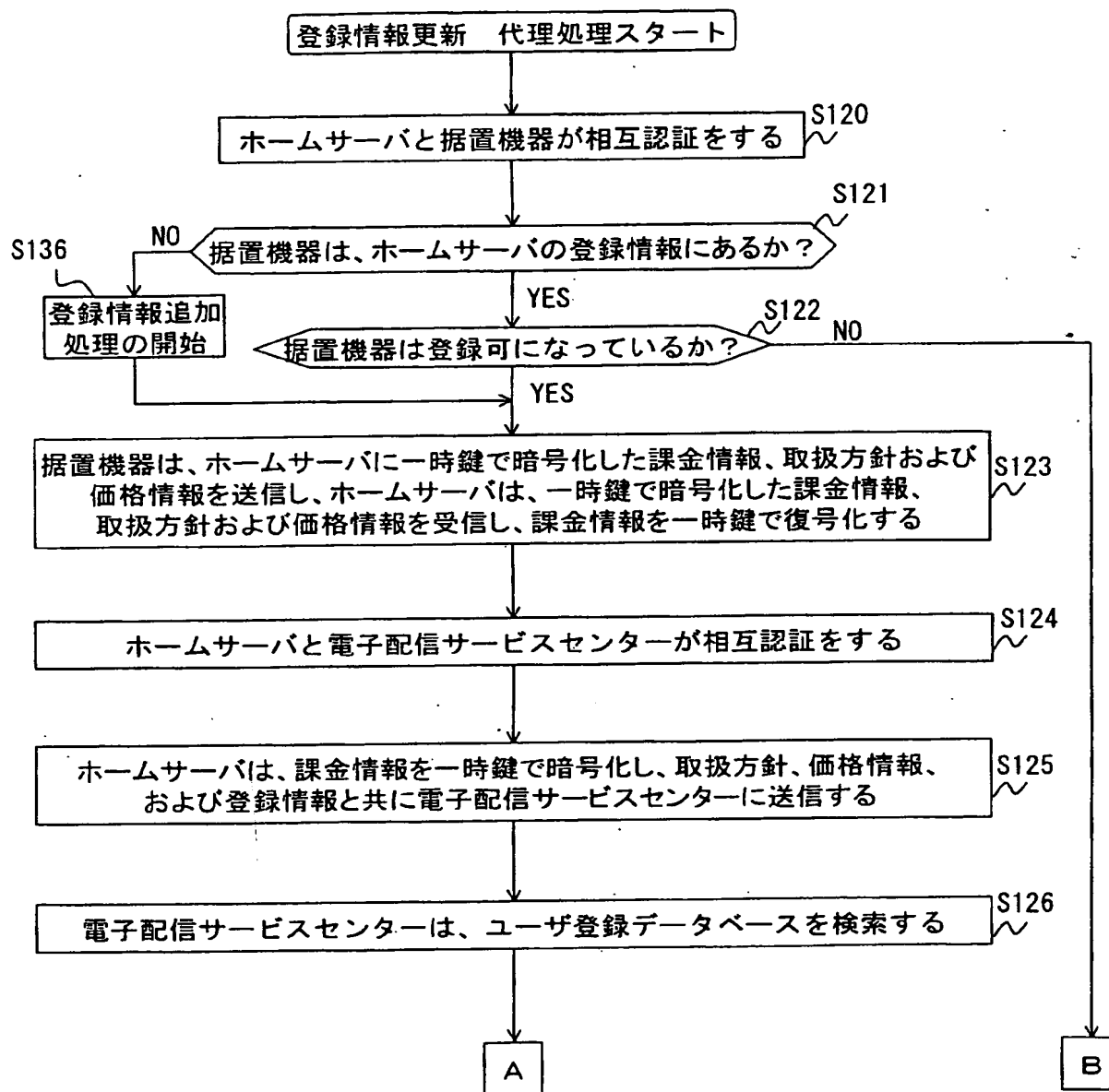


図 6 3

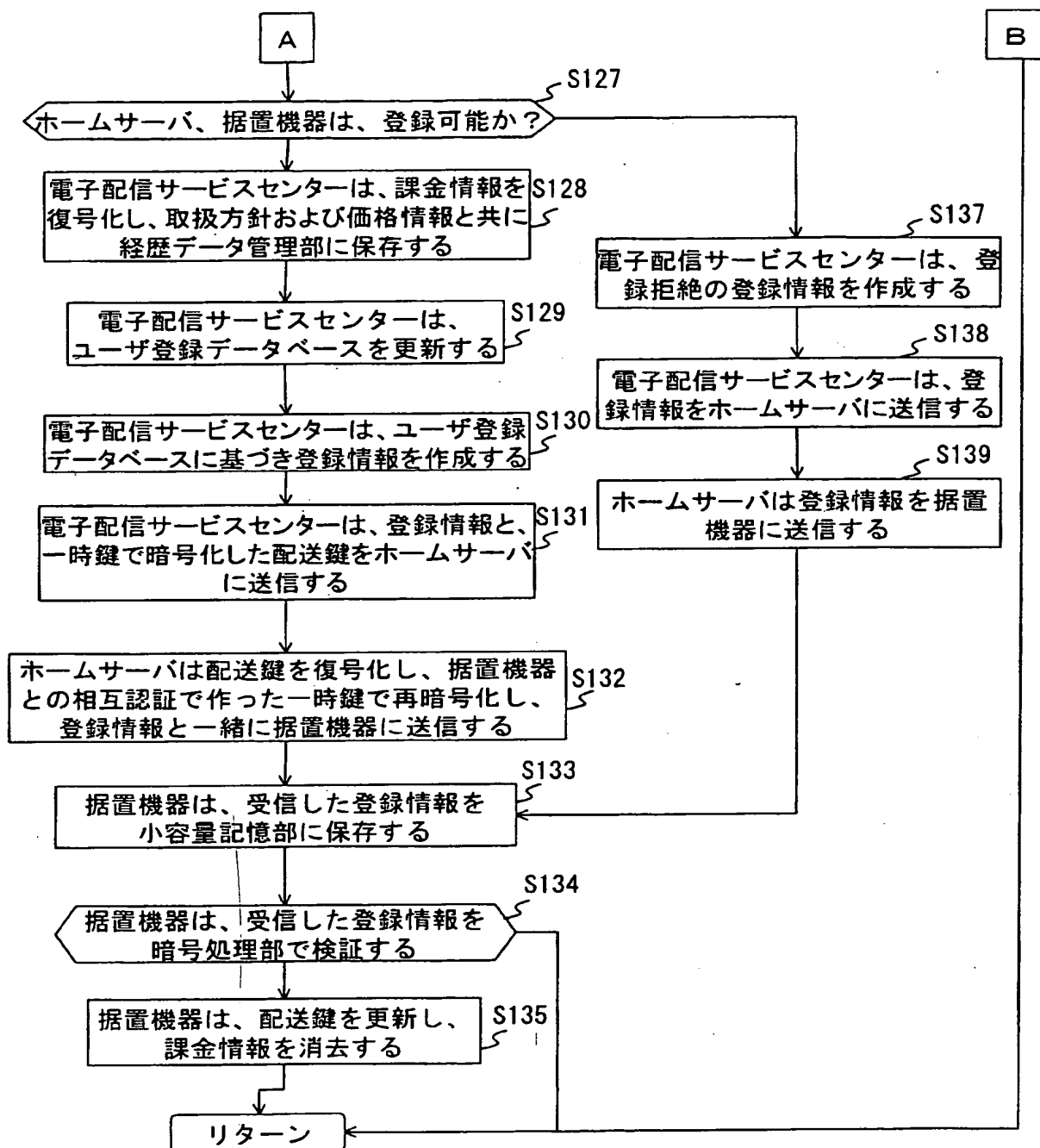


図 6 4

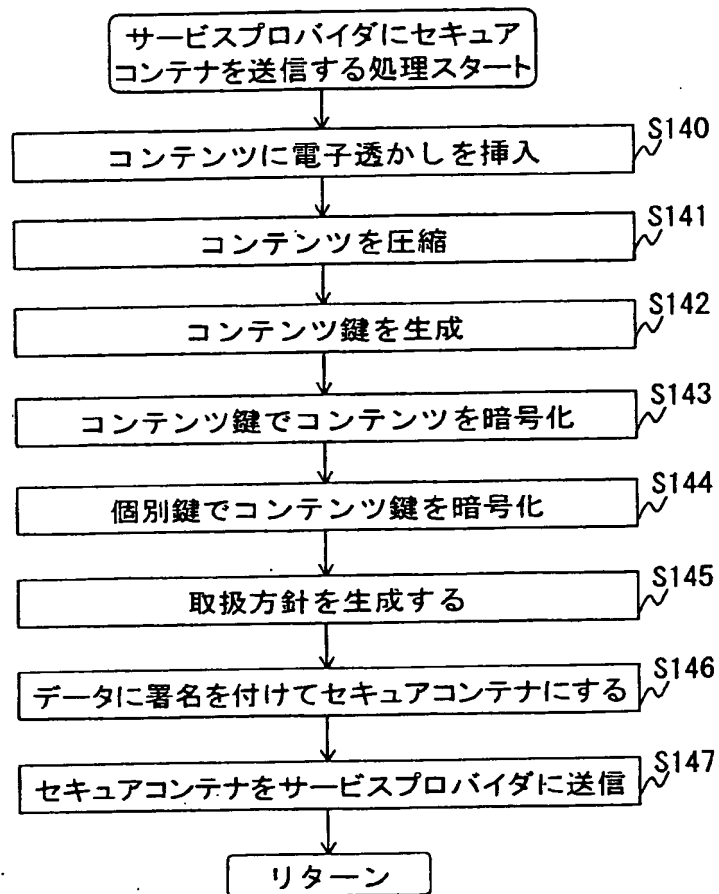


図 6 5



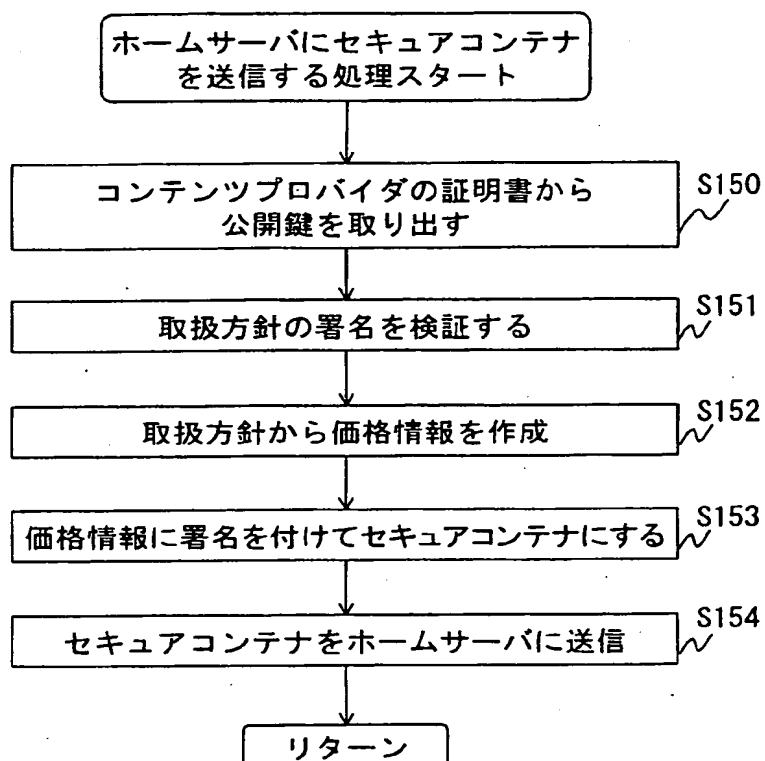


図 6 6

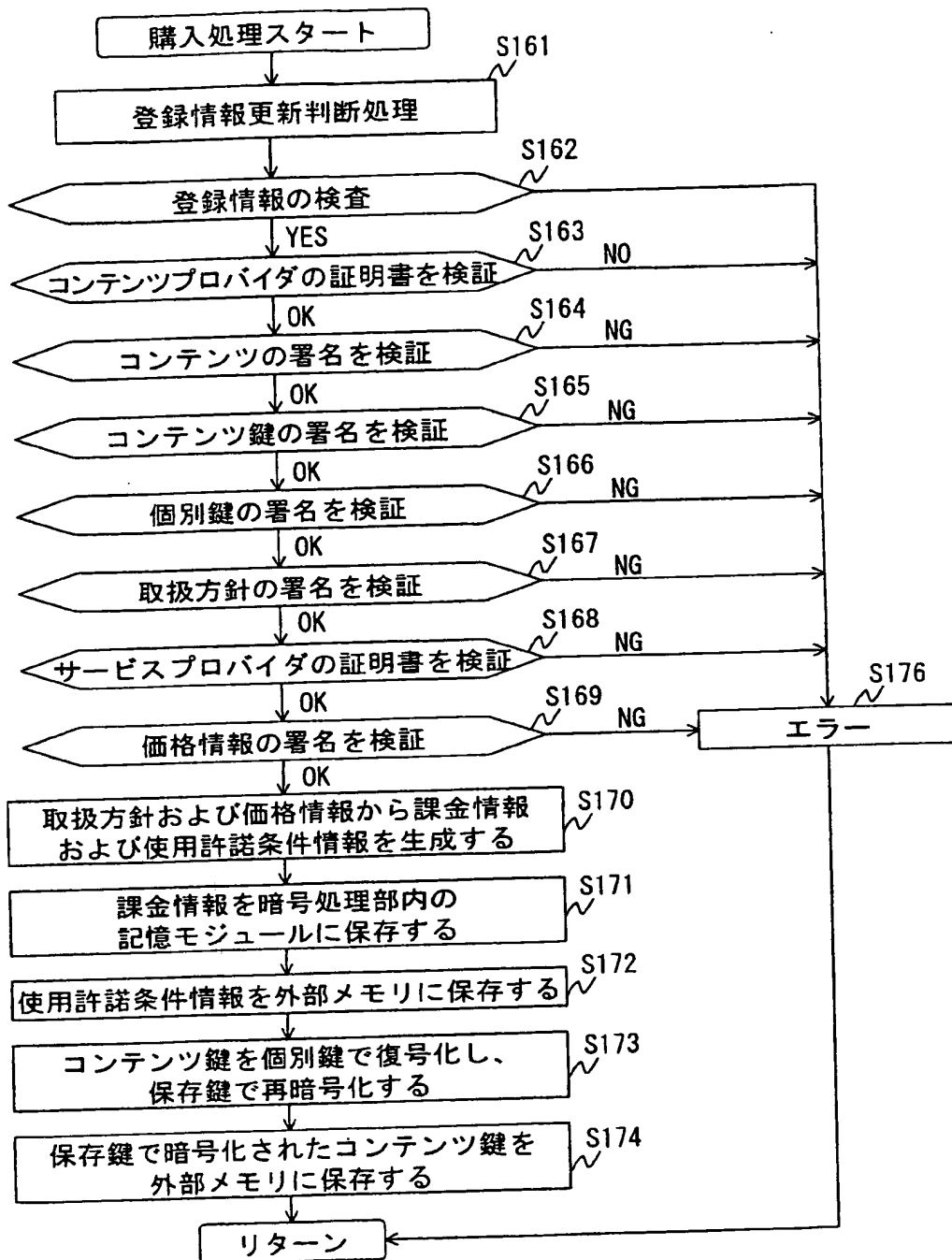


図 67

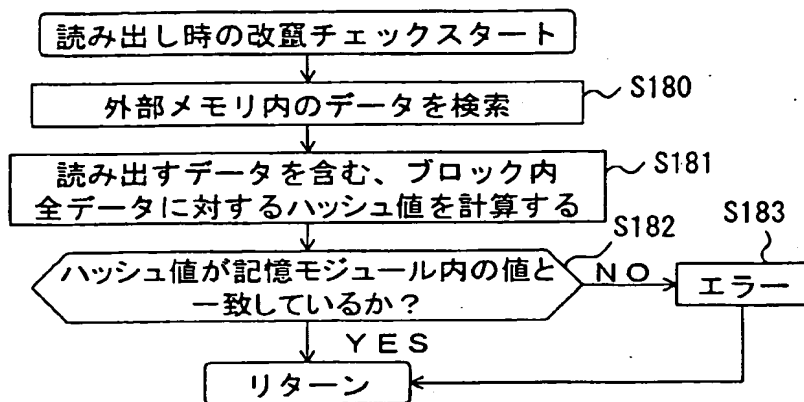


図 6 8

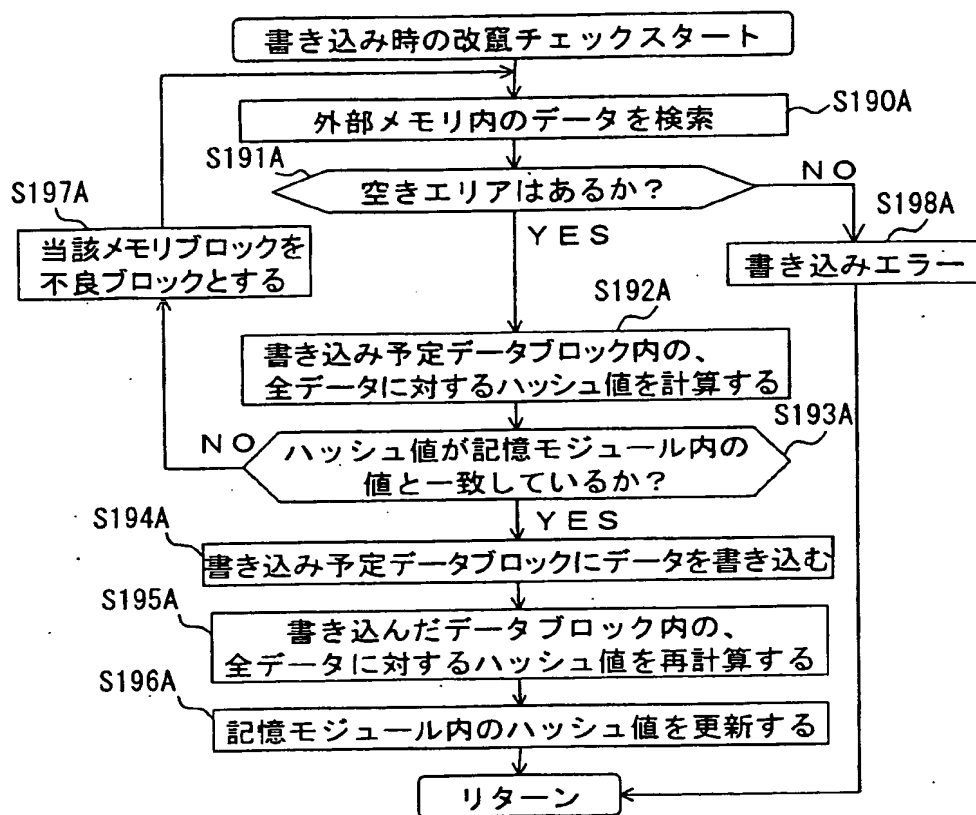


図 6 9

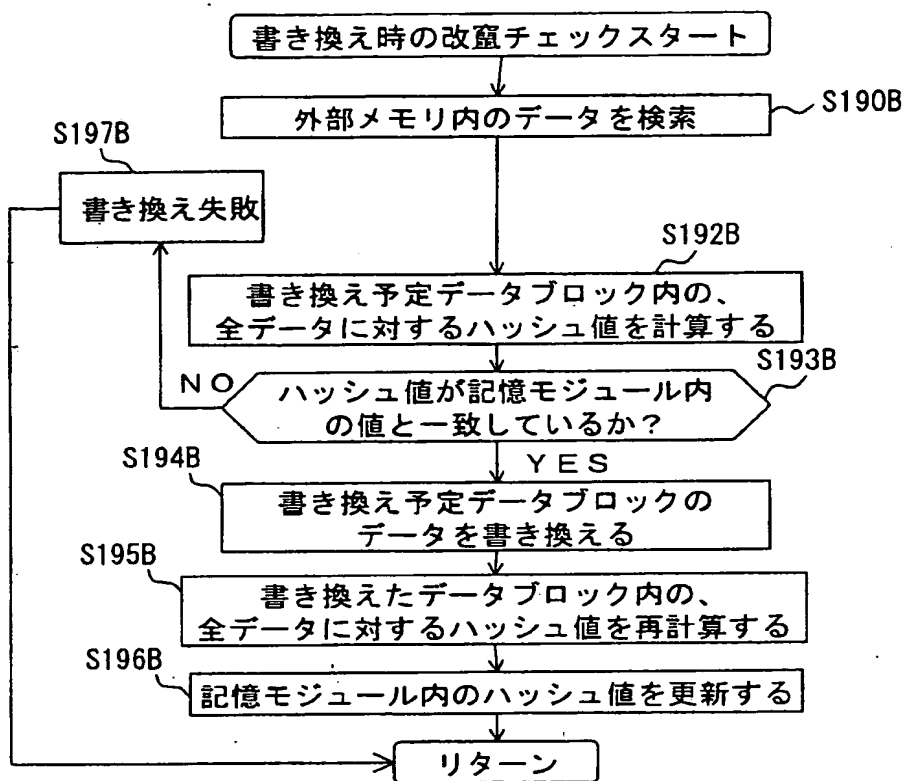


図 70

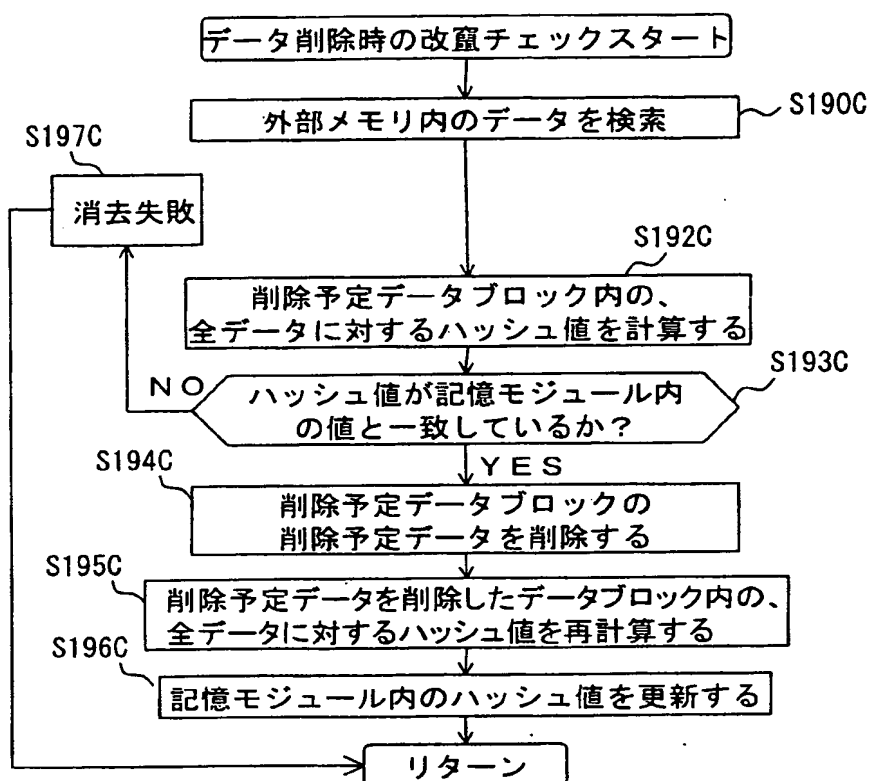


図 7 1

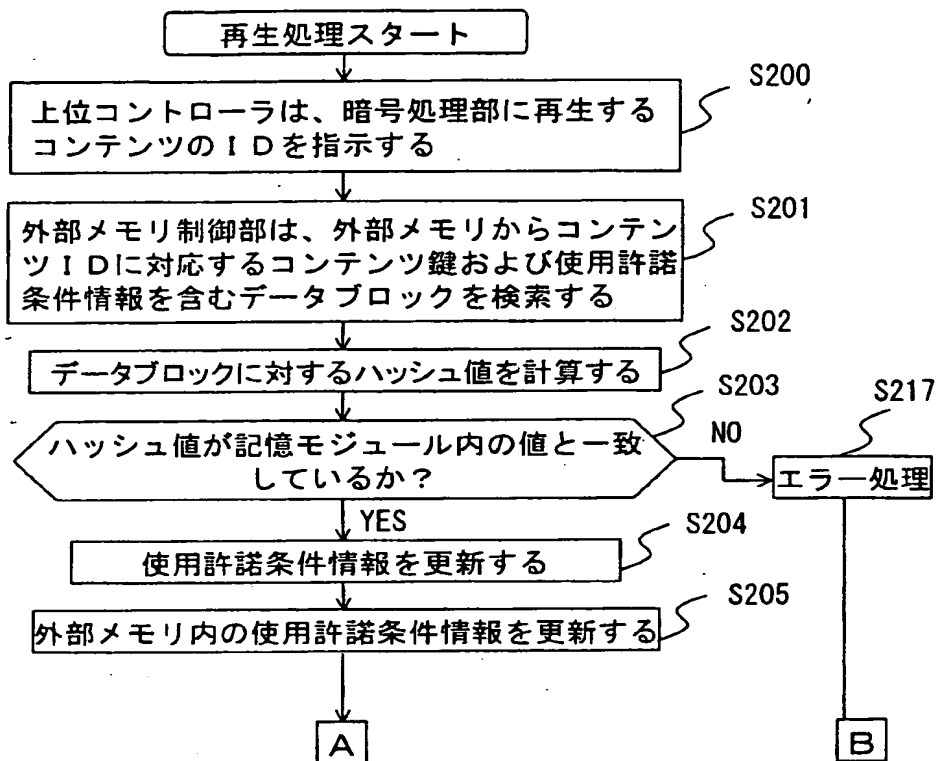


図 7 2

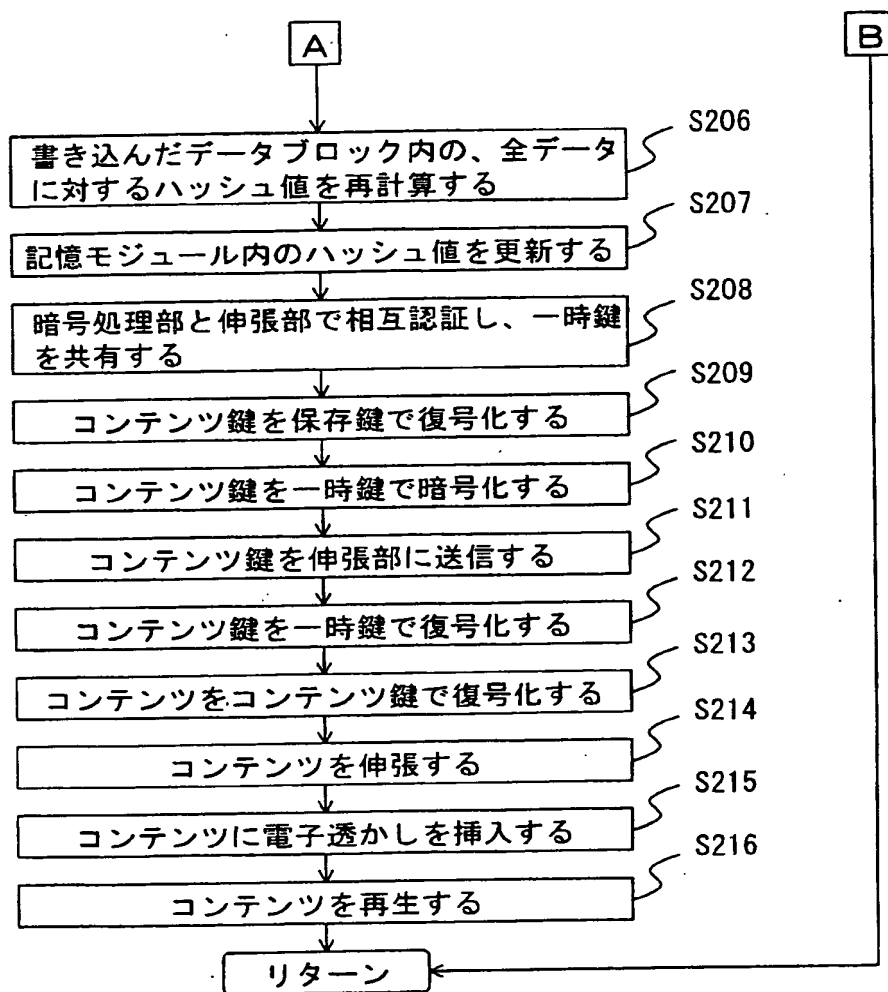


図 7 3



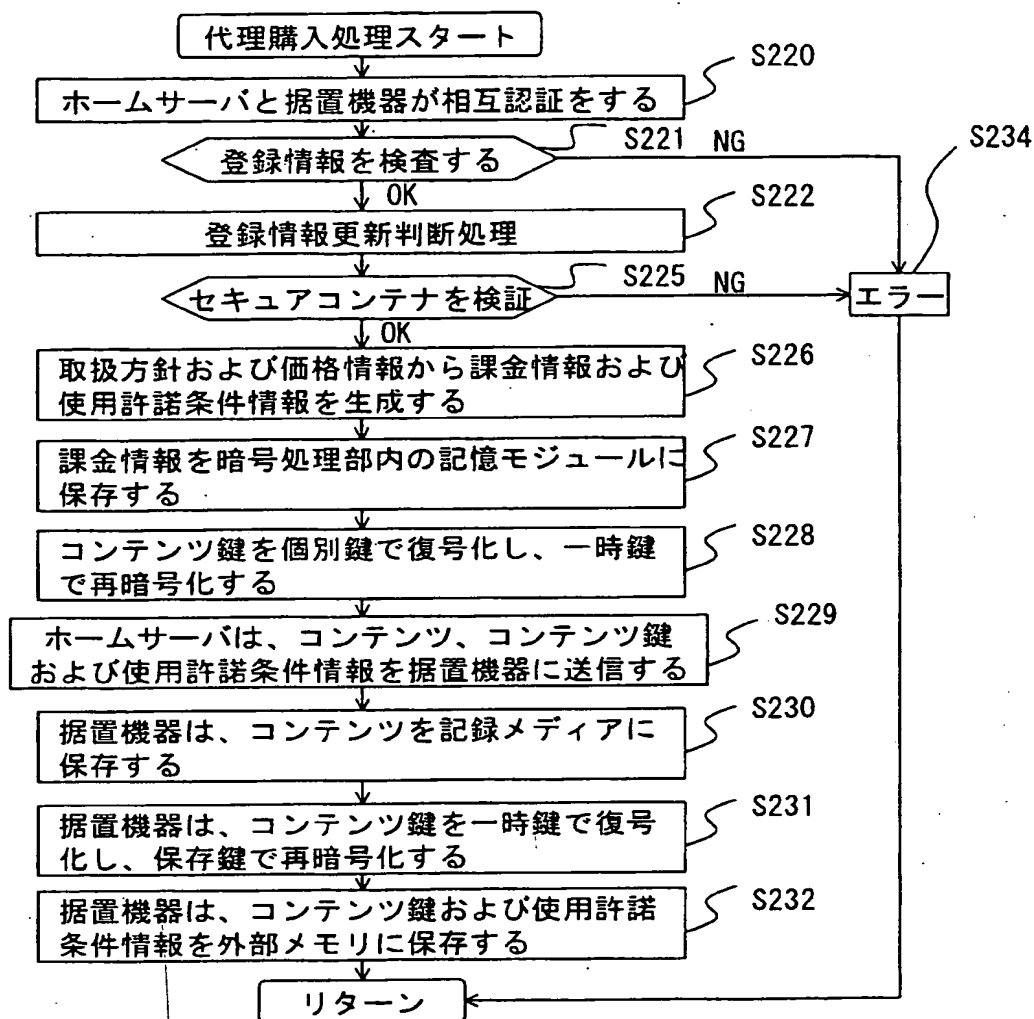


図 7 4

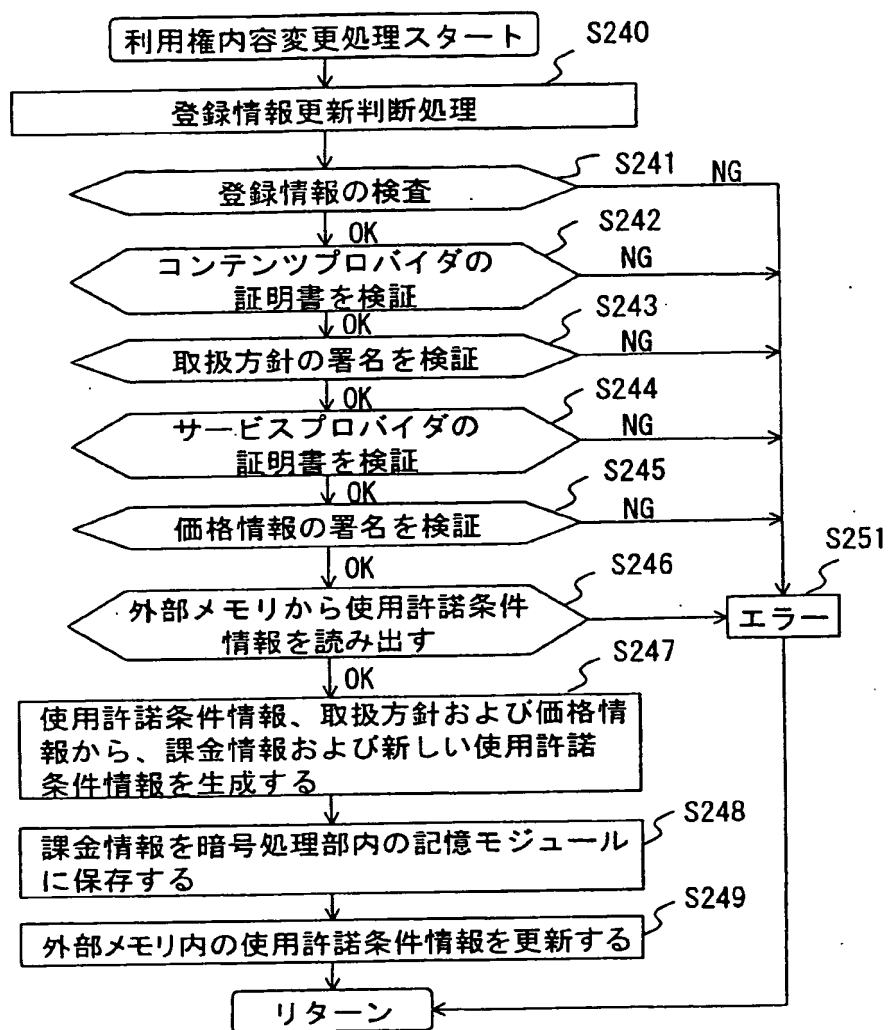


図 7 5

ルール n	ルール番号
	利用権内容番号
	パラメータ
	最低価格
	取り分（利益率）
ルール 1	ルール番号 # 1
	利用権内容番号 # 1
	なし
	¥ 3 5 0
	3 0 %
ルール 2	ルール番号 # 2
	利用権内容番号 # 2
	1 時間
	¥ 1 0 0
	3 0 %
ルール 3	ルール番号 # 3
	利用権内容番号 # 6
	1 回
	¥ 3 0
	3 0 %
ルール 4	ルール番号 # 4
	利用権内容番号 # 1 3
	# 2 / # 1
	¥ 2 0 0
	2 0 %
ルール 5	ルール番号 # 5
	利用権内容番号 # 1 4
	# 1 / # 1
	¥ 2 5 0
	2 0 %

図 7 6

ルール n	ルール番号
	パラメータ
	価格
ルール 1	ルール番号# 1
	3 0 %
	¥ 5 0 0
ルール 2	ルール番号# 2
	4 0 %
	¥ 1 0 0
ルール 3	ルール番号# 3
	4 0 %
	¥ 1 0 0
ルール 4	ルール番号# 4
	1 0 %
	¥ 2 0 0
ルール 5	ルール番号# 5
	2 0 %
	¥ 3 5 0

図 7 7

ルール 1	# 1
	# 1
	なし
	¥ 3 5 0
	3 0 %
ルール 2	# 2
	# 2
	1 時間
	¥ 1 0 0
	3 0 %
ルール 3	# 3
	# 1 3
	# 2 / # 1
	¥ 2 0 0
	2 0 %

取扱方針のルール部の一部

ルール 1	# 1
	3 0 %
	¥ 5 0 0
ルール 2	# 2
	4 0 %
	¥ 1 0 0
ルール 3	# 3
	1 0 %
	¥ 2 0 0

価格情報のルール部の一部

現在

ルール	ルール番号
	利用権内容番号
	パラメータ
ルール	# 2
	# 2
	3 0 分 / 2 時間

使用許諾条件情報のルール部

変更後

ルール	ルール番号
	利用権内容番号
	パラメータ
ルール	# 1
	# 1
	なし

使用許諾条件情報のルール部

図 7 8

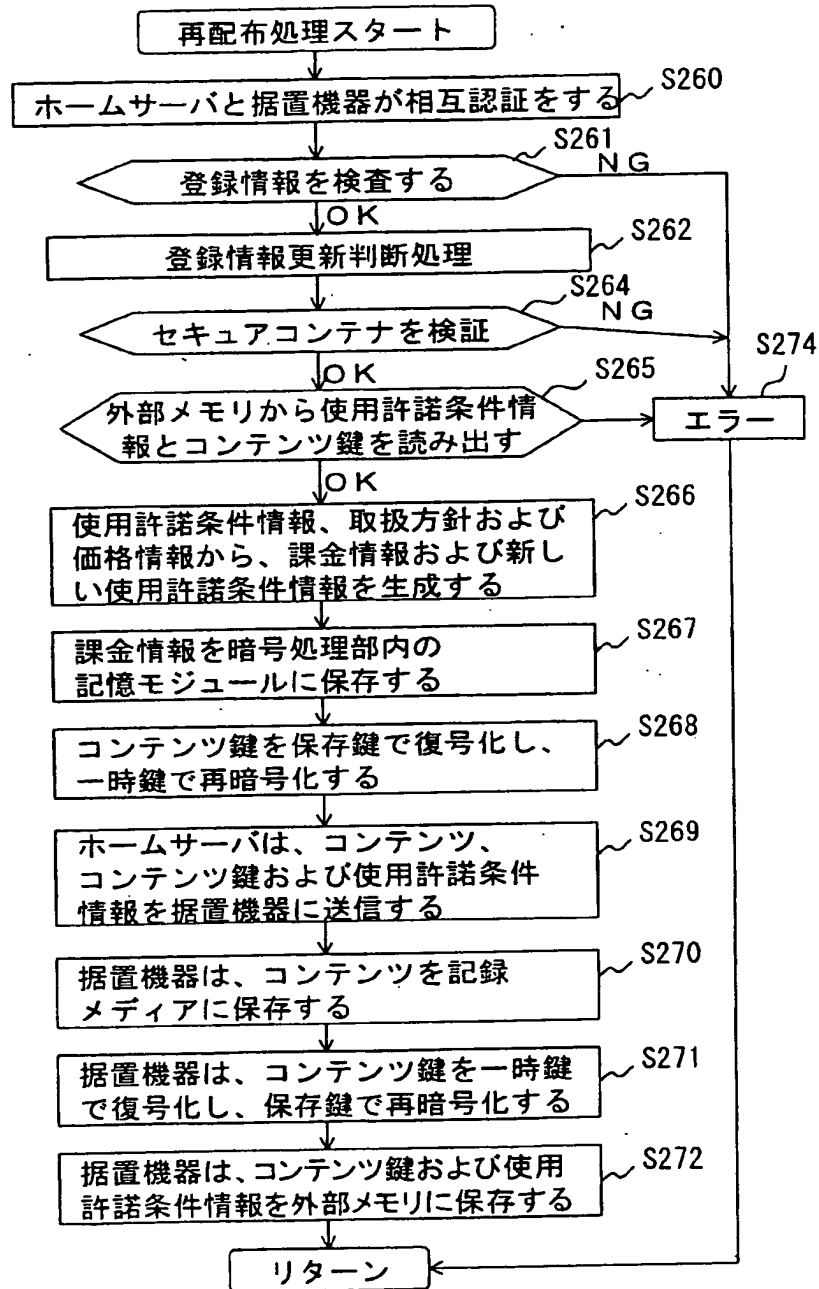


図 7 9

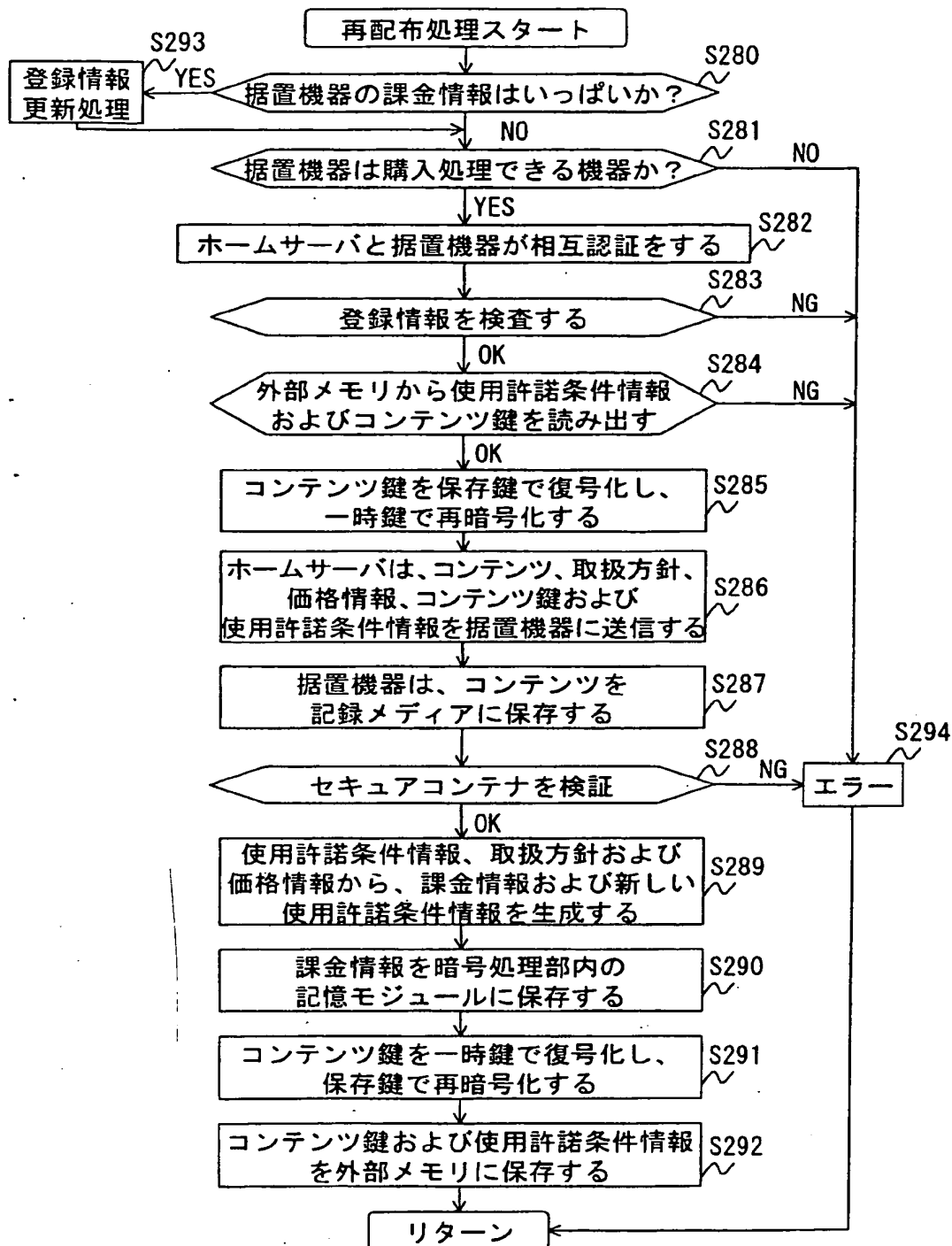


図 80

ル ー ル 1	ルール番号 # 1
	利用権内容番号 # 1
	なし
	¥ 3 5 0
	3 0 %
ル ー ル 2	ルール番号 # 2
	利用権内容番号 # 1 6
	なし
	¥ 1 0 0
	5 0 %

取扱方針のルール部の一部

ル ー ル 1	ルール番号 # 1
	3 0 %
	¥ 5 0 0
ル ー ル 2	ルール番号 # 2
	0 %
	¥ 1 0 0

価格情報のルール部の一部

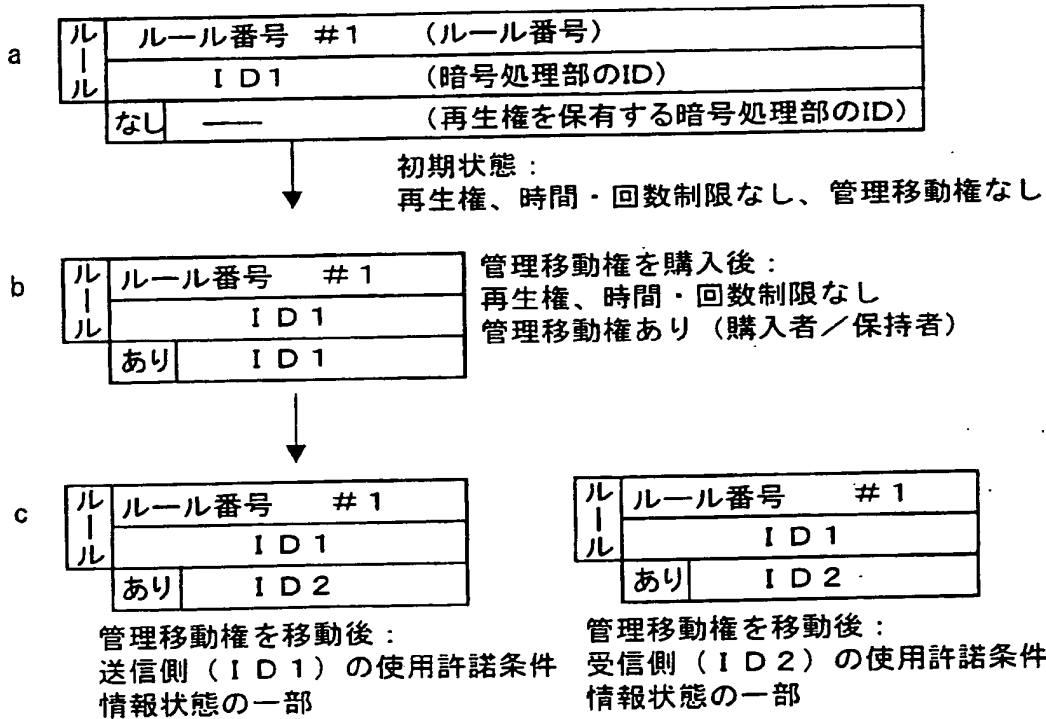


図 8 1



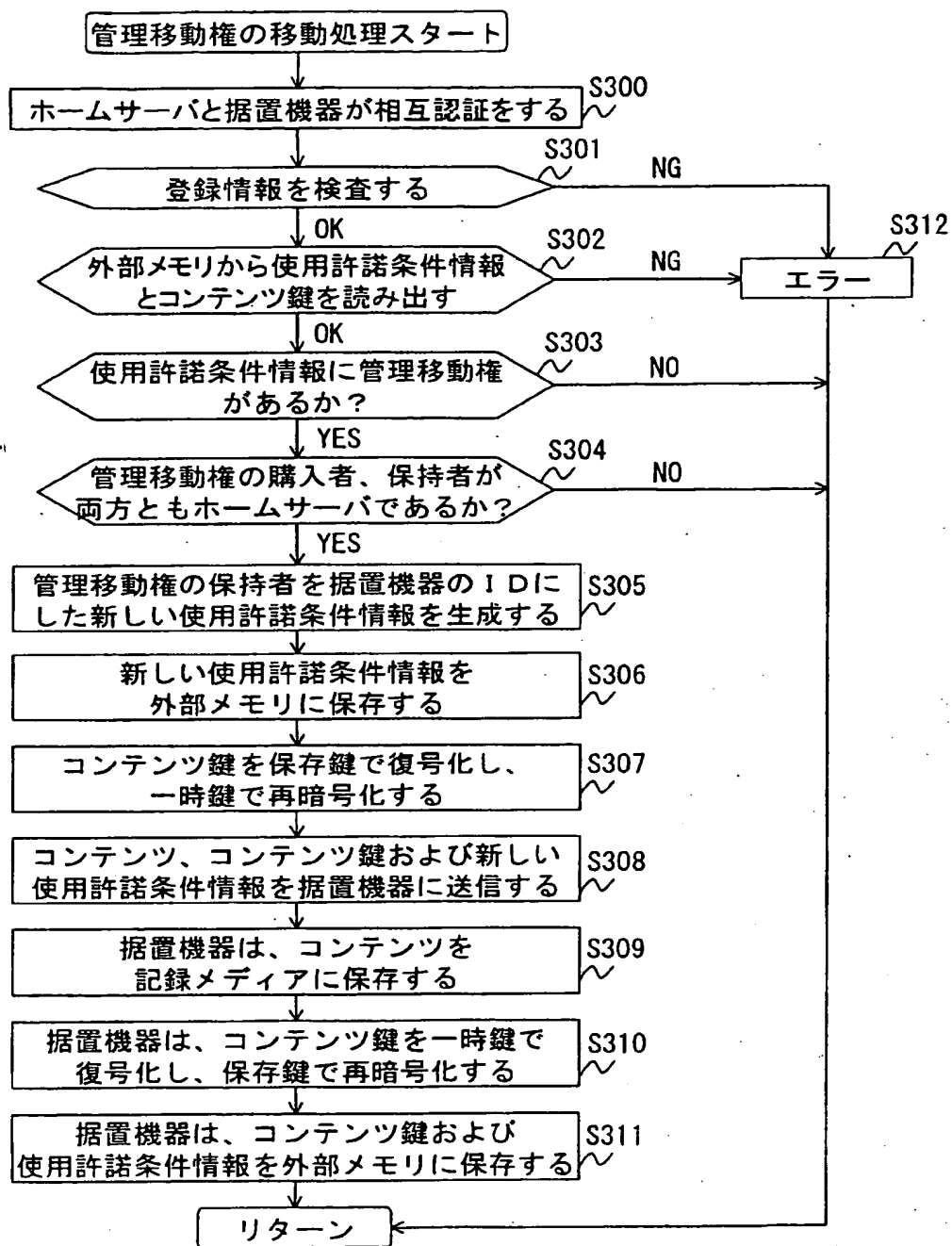


図 8 2

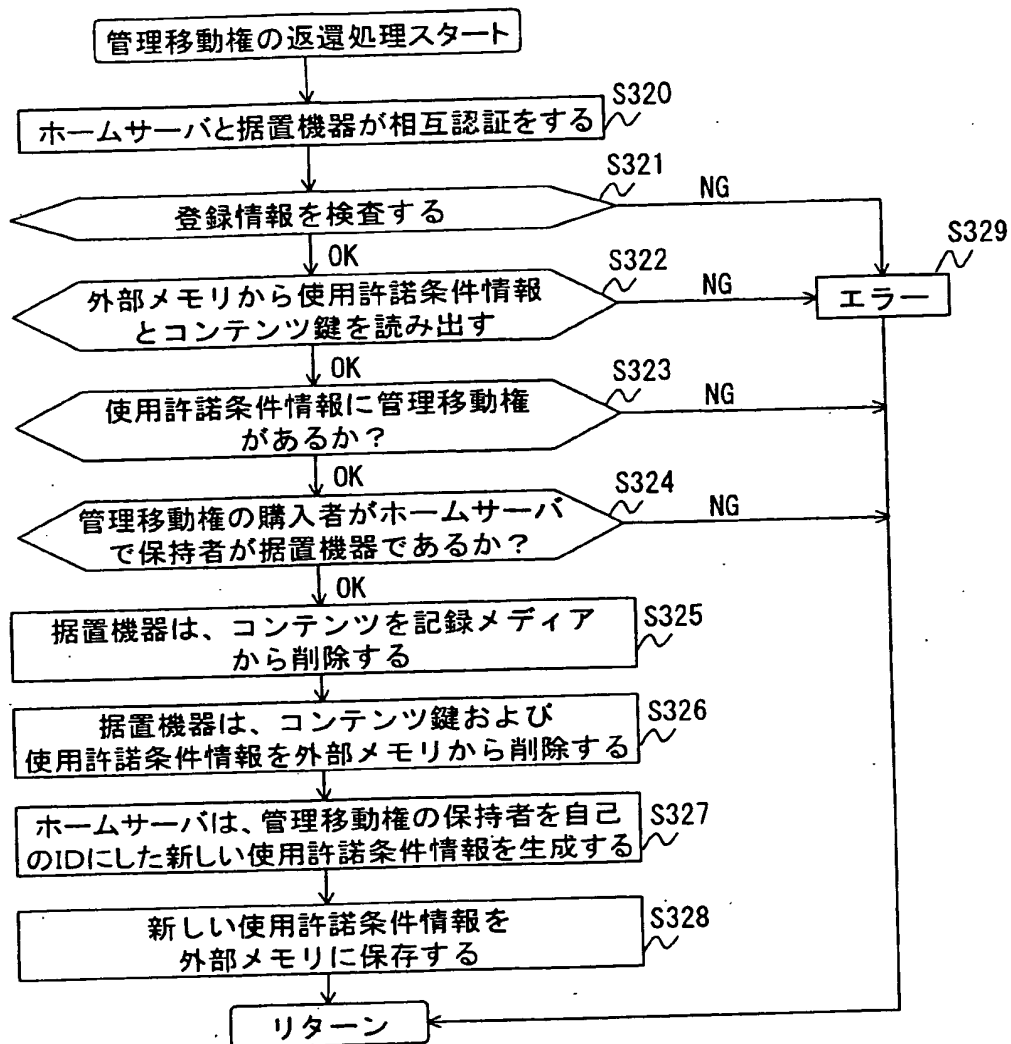


図 8 3

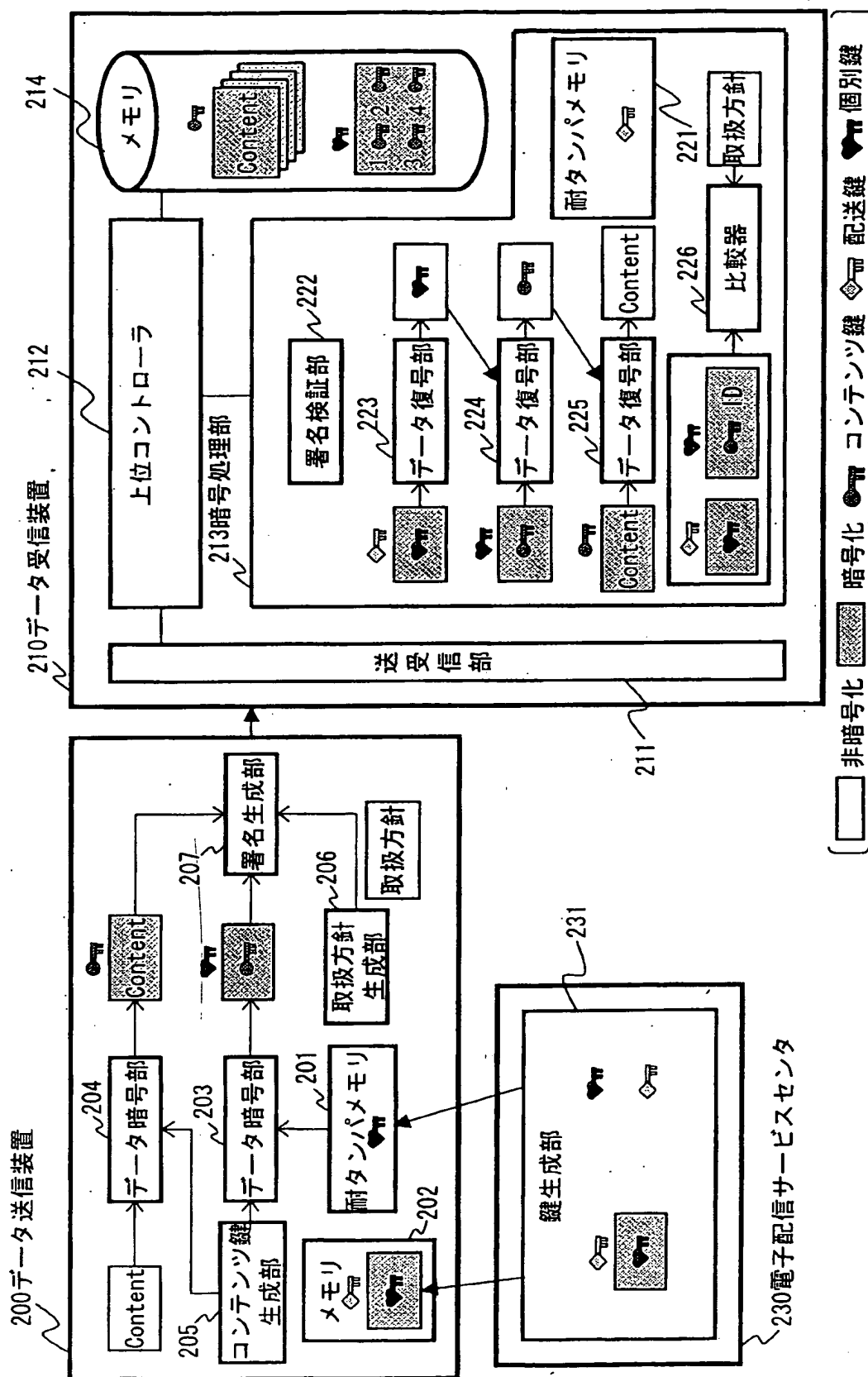


図84

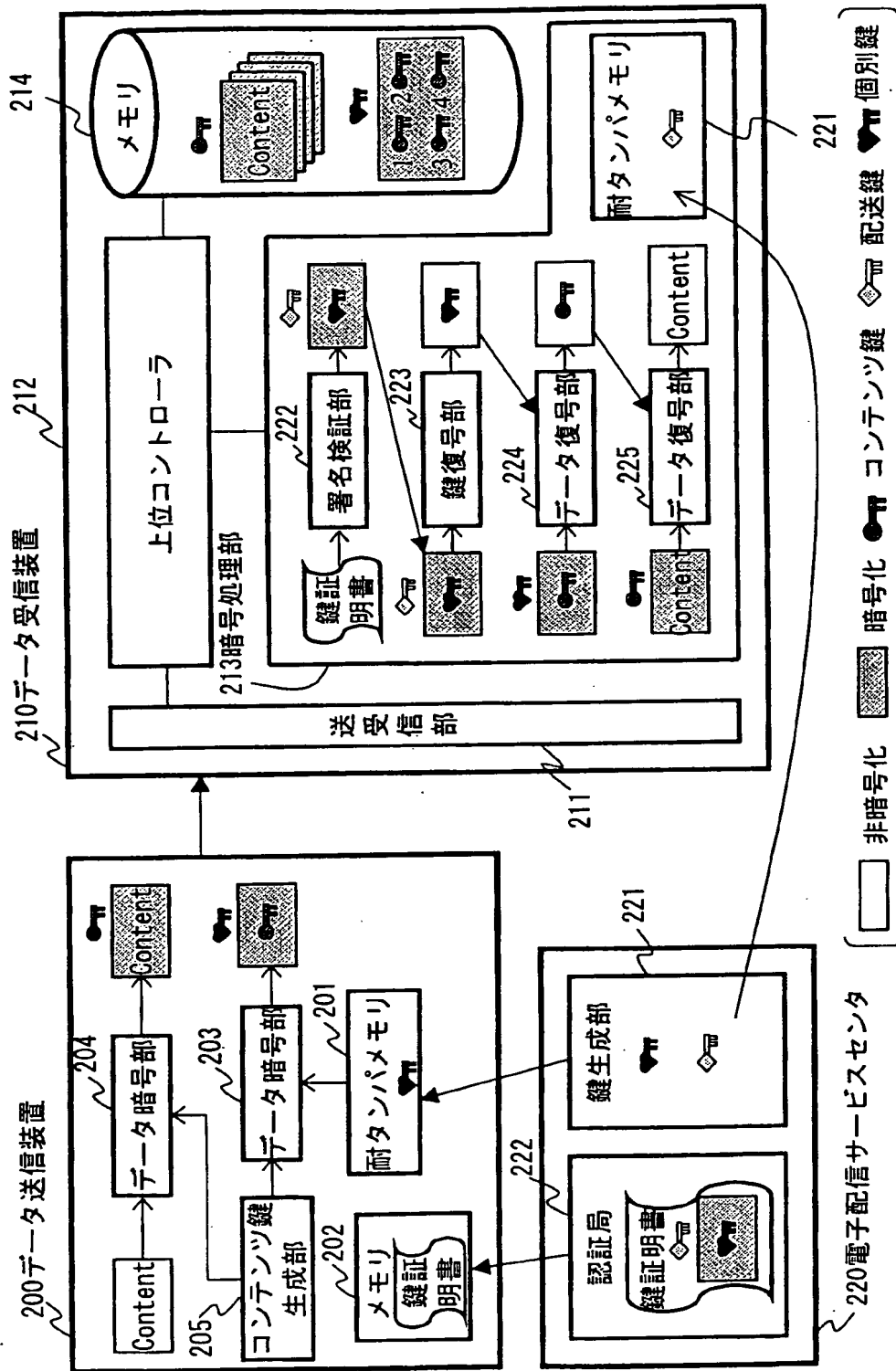


図 8 5

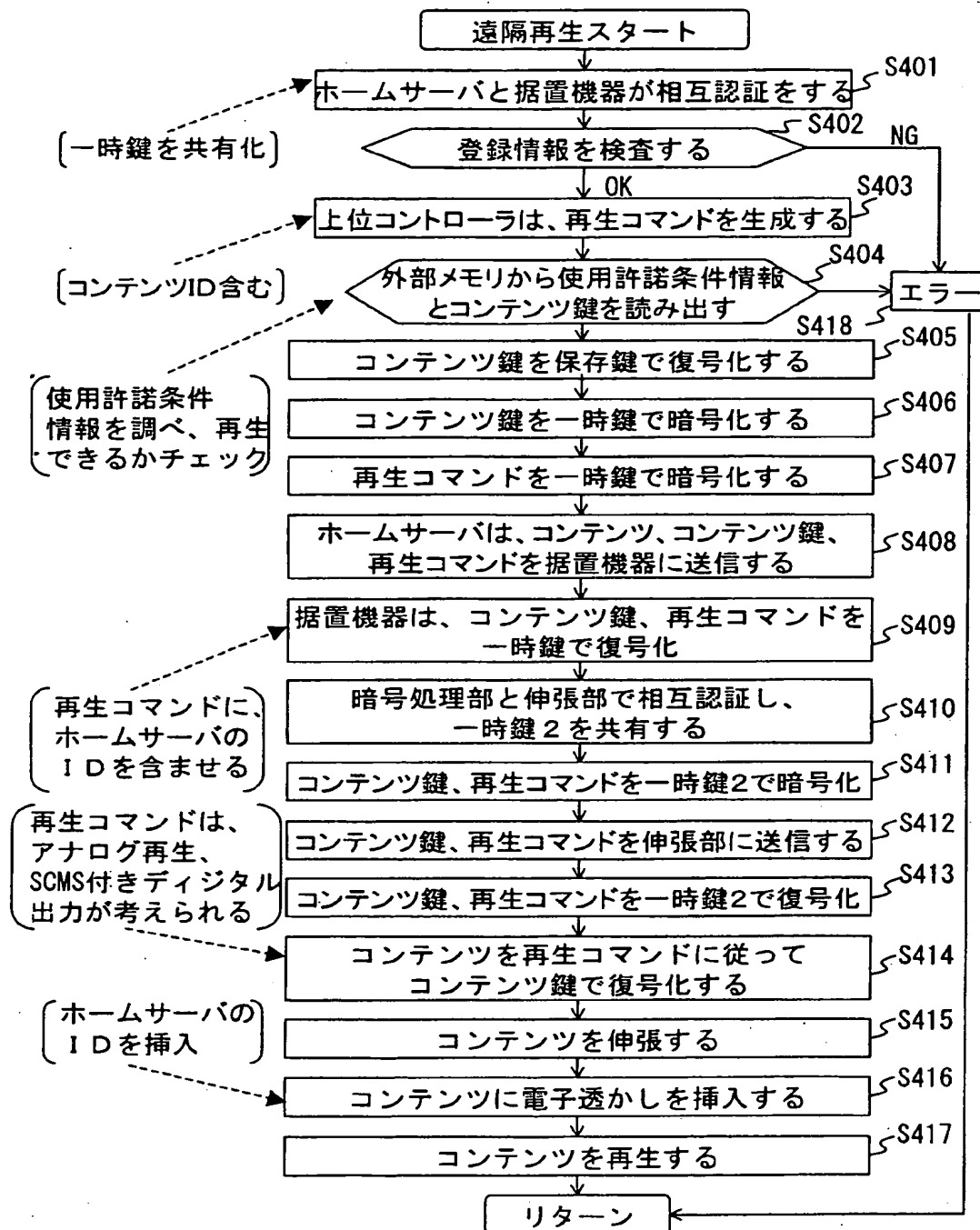


図 86

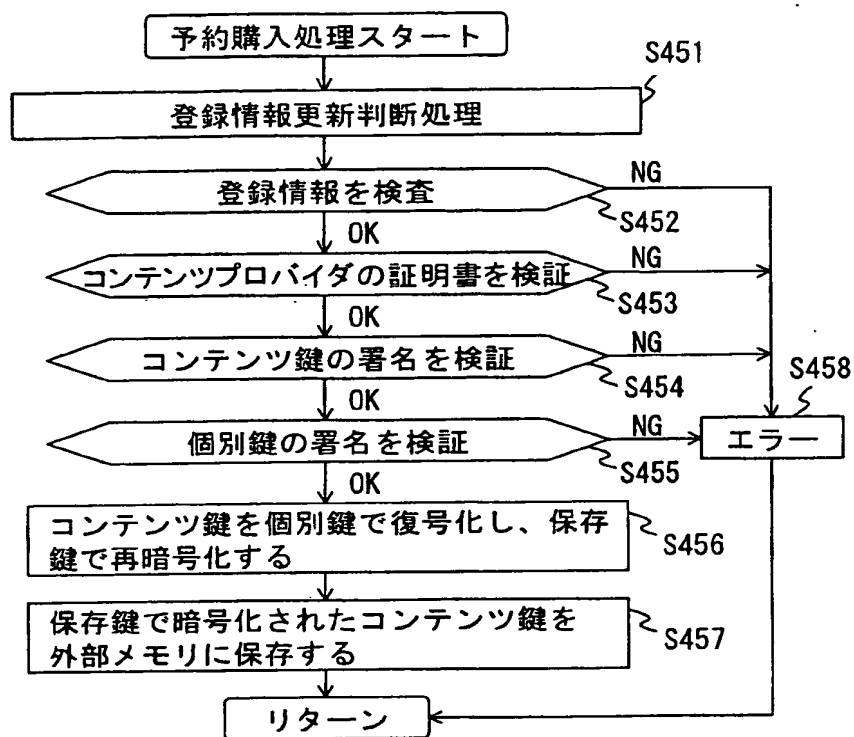


図 8 7

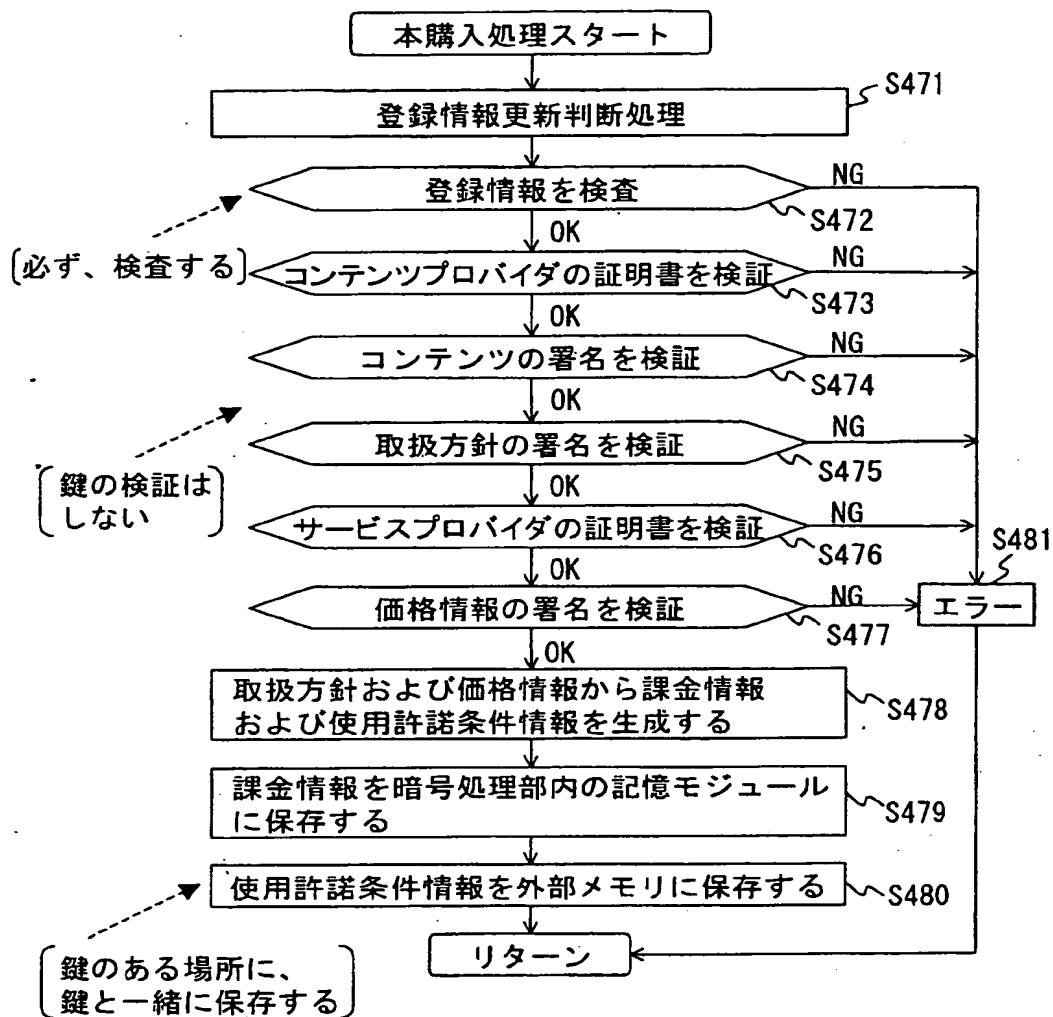


図 8 8

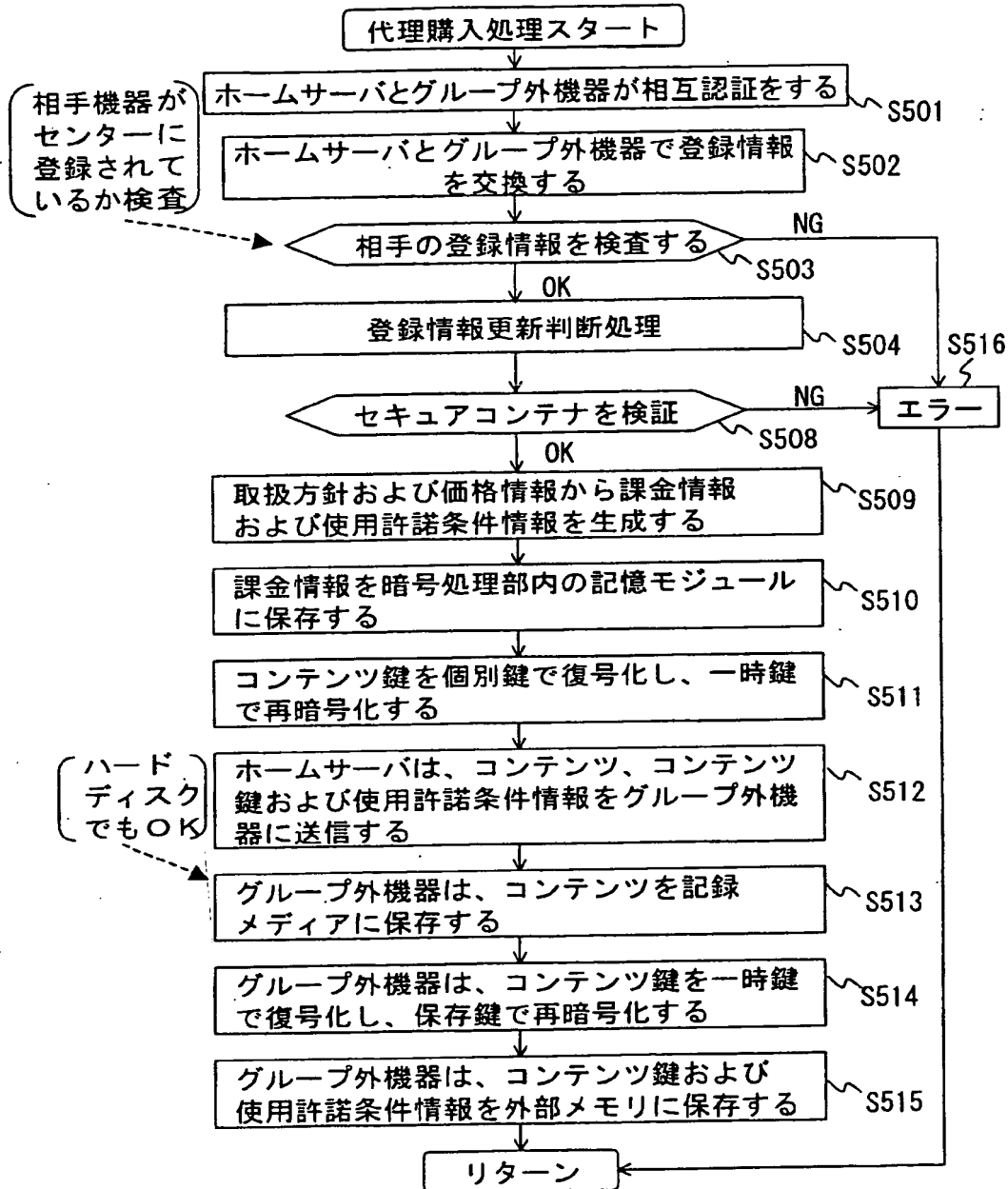


図 8 9



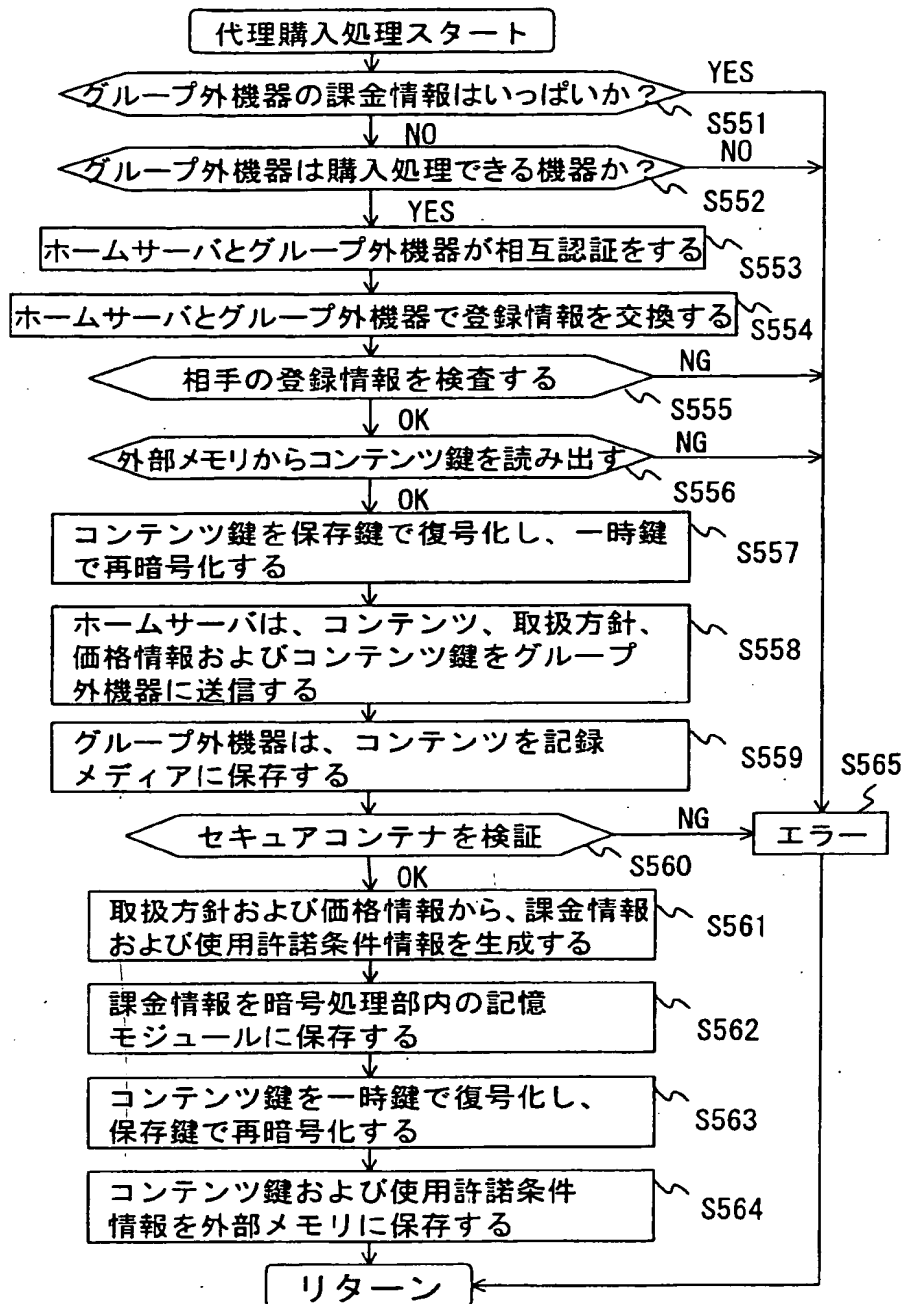


図 90

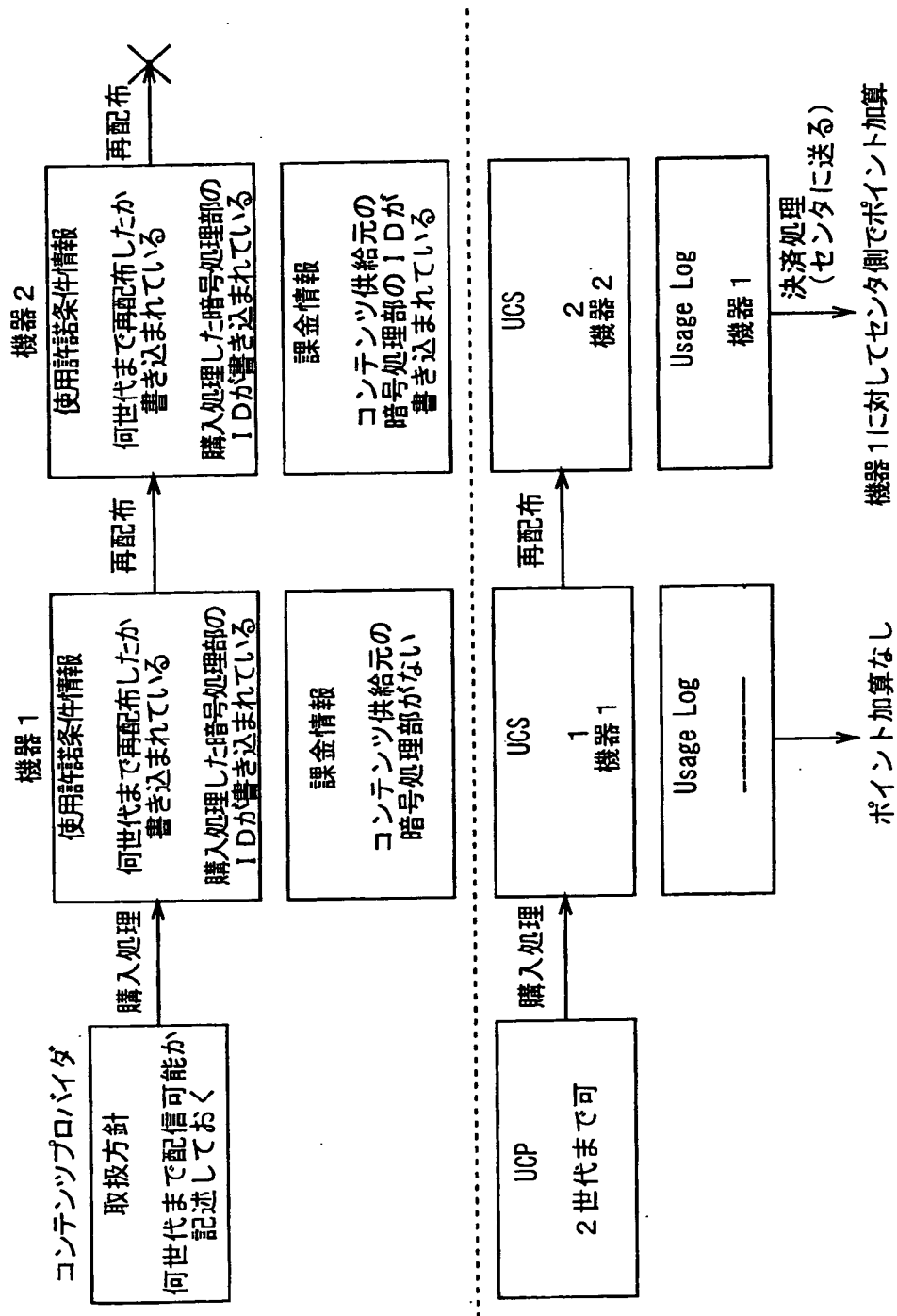


図91

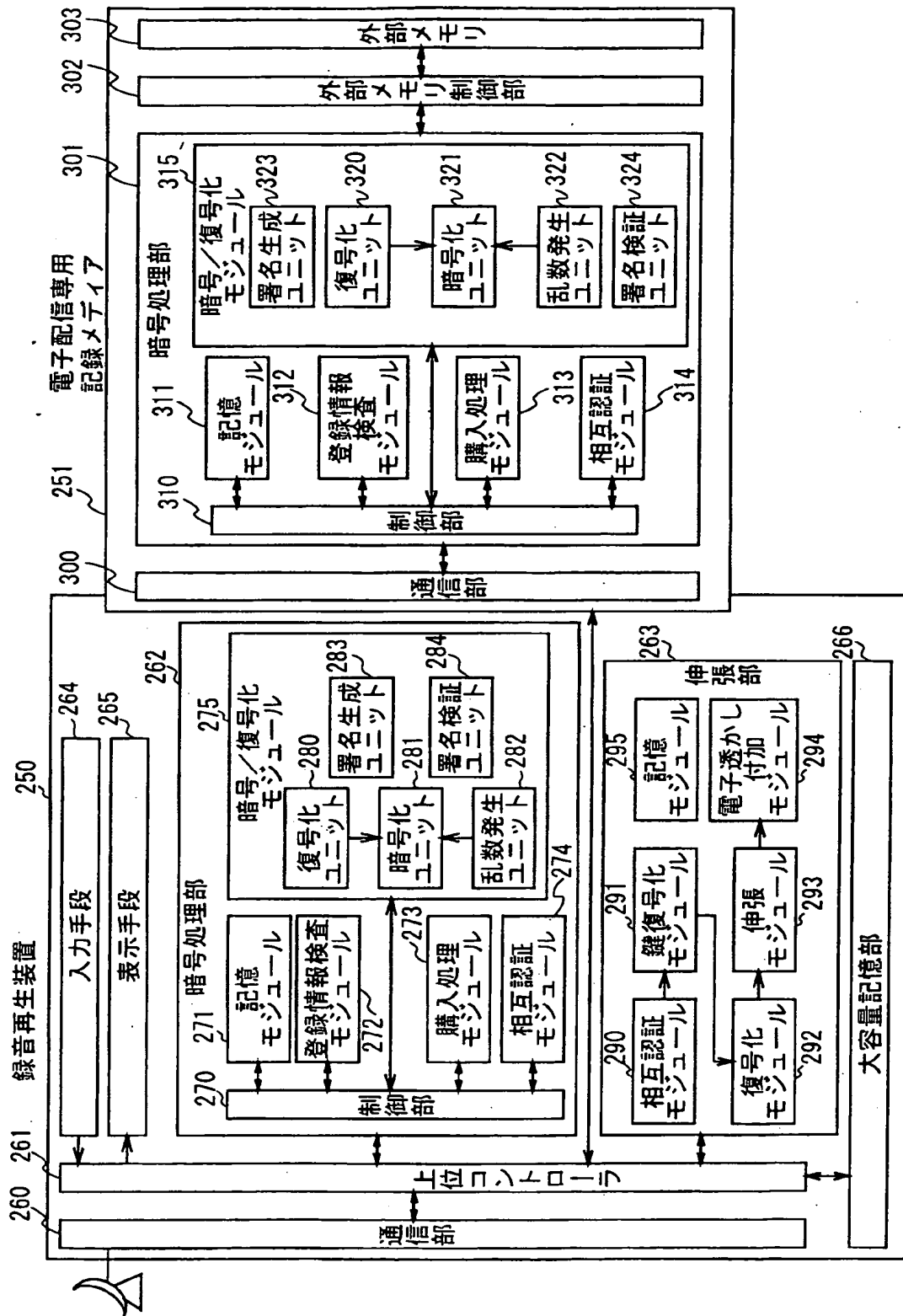


図 9 2

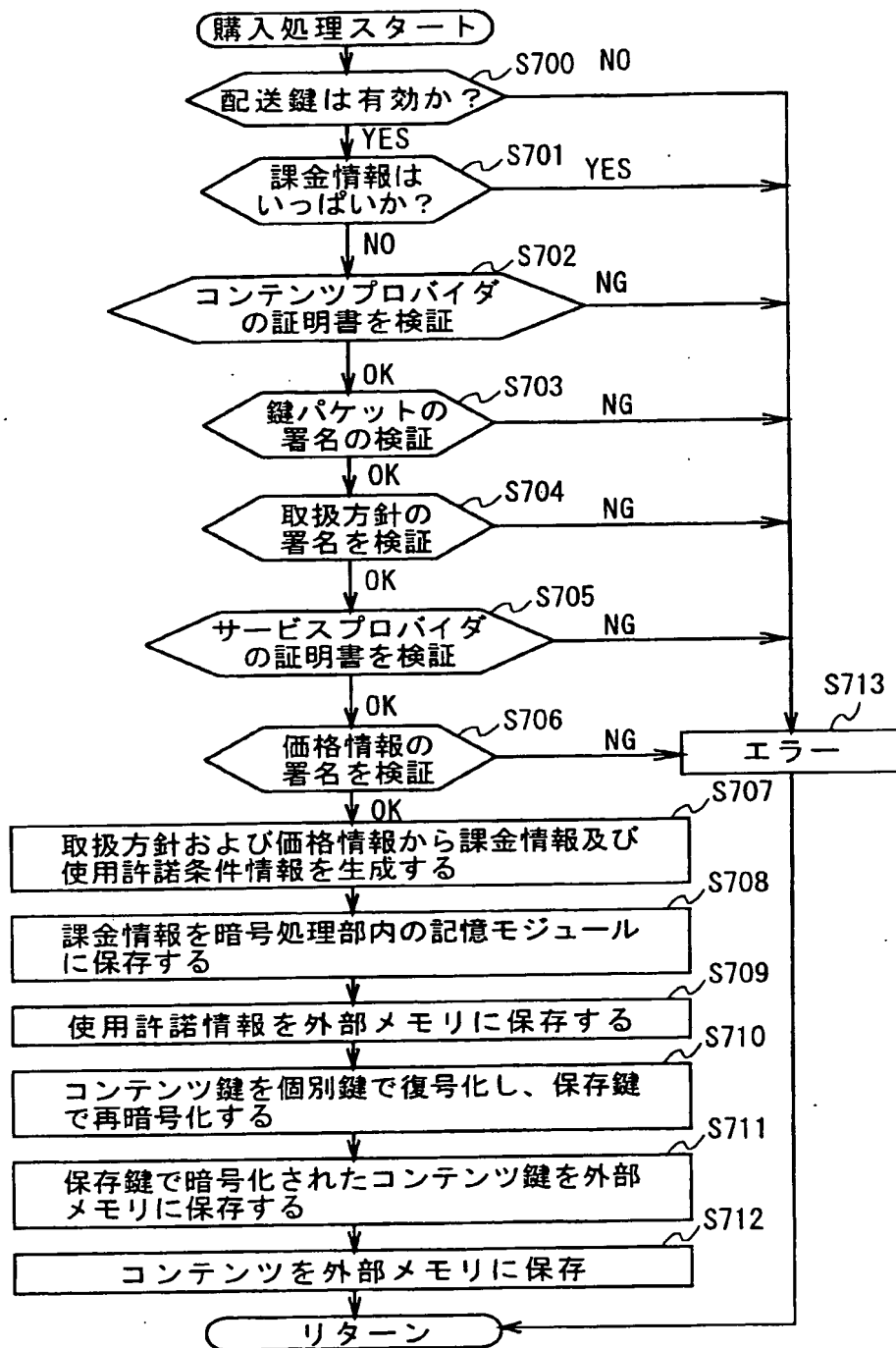


図 9 3

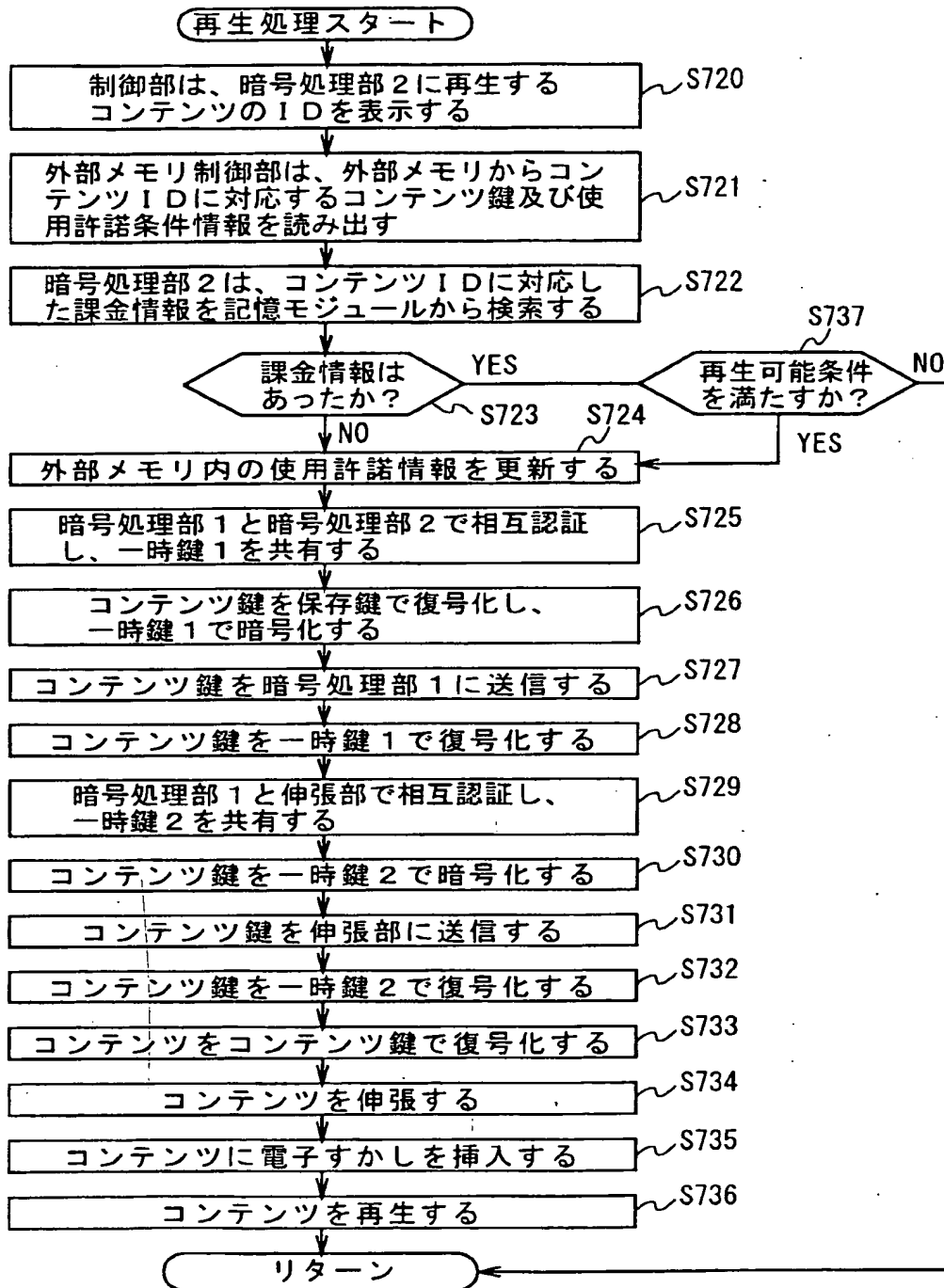


図 9 4

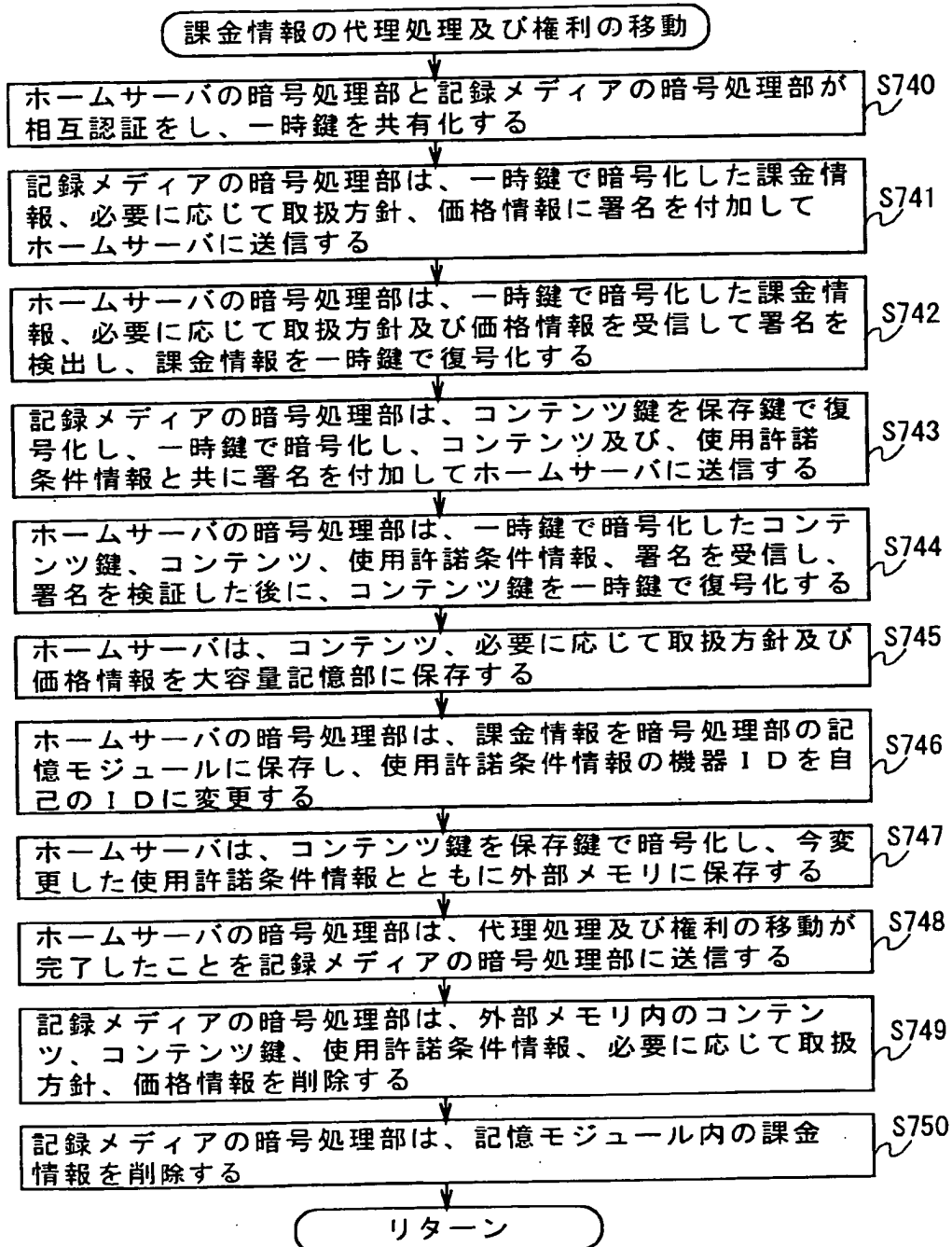


図 9 5

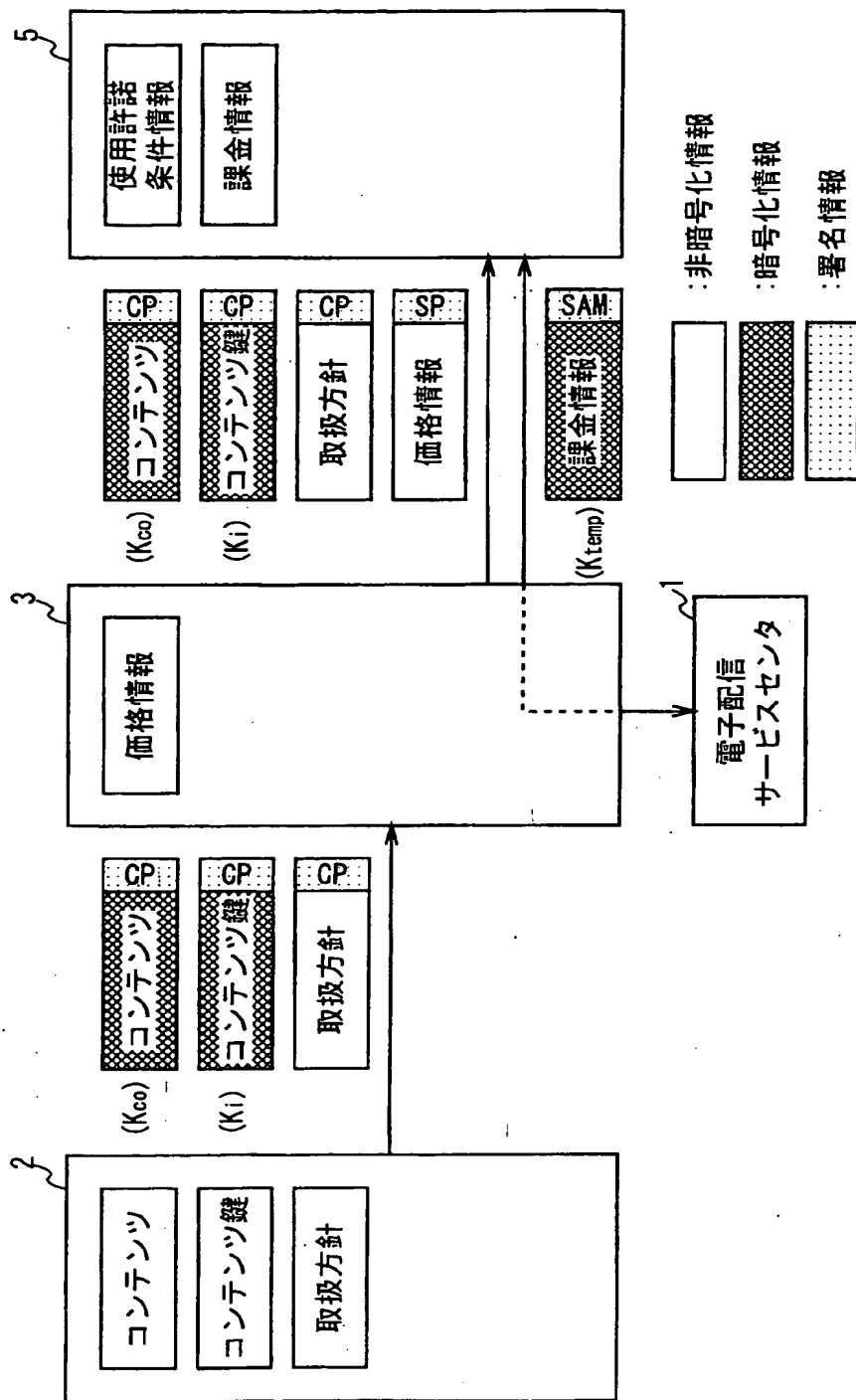


図 9 6

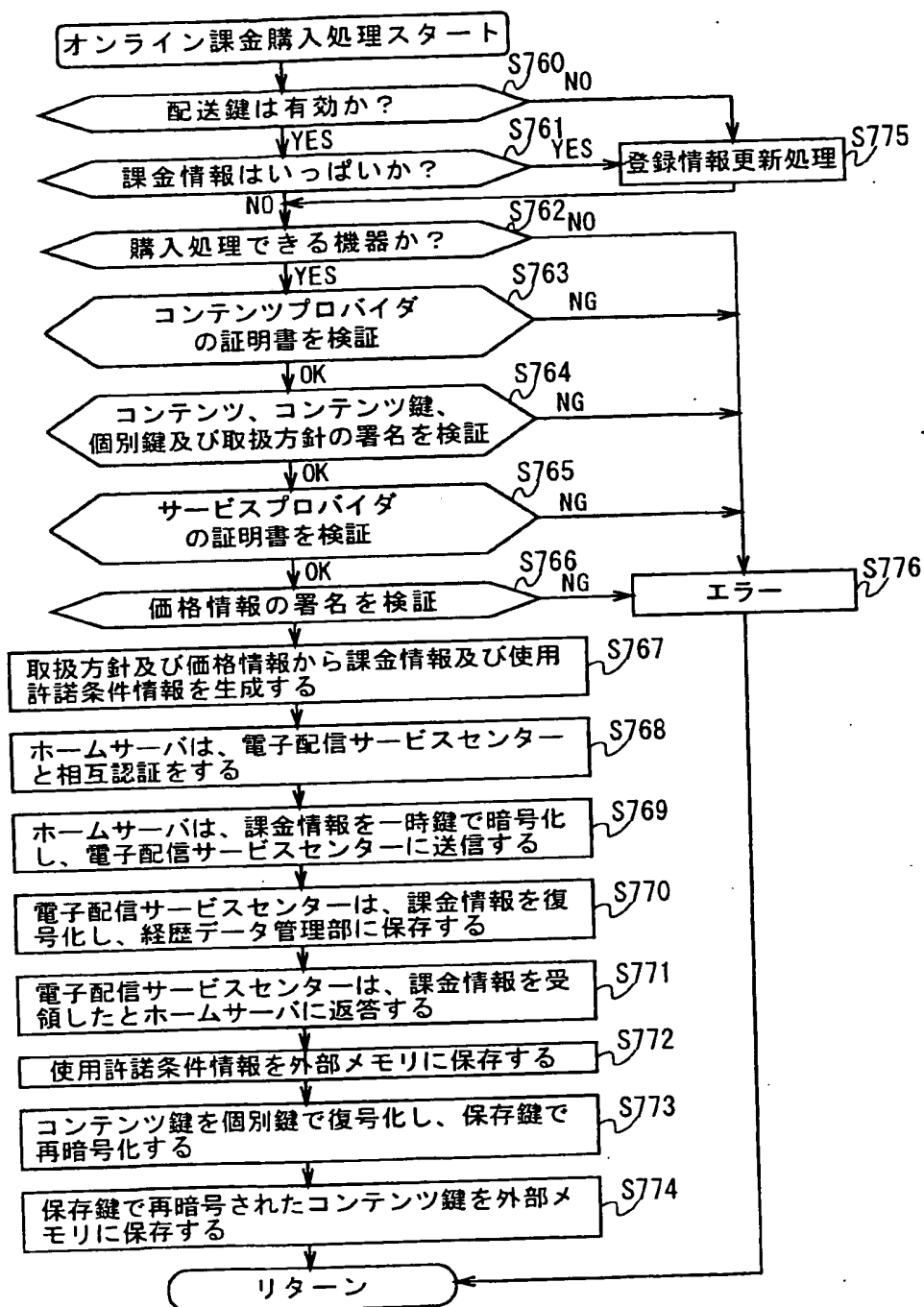
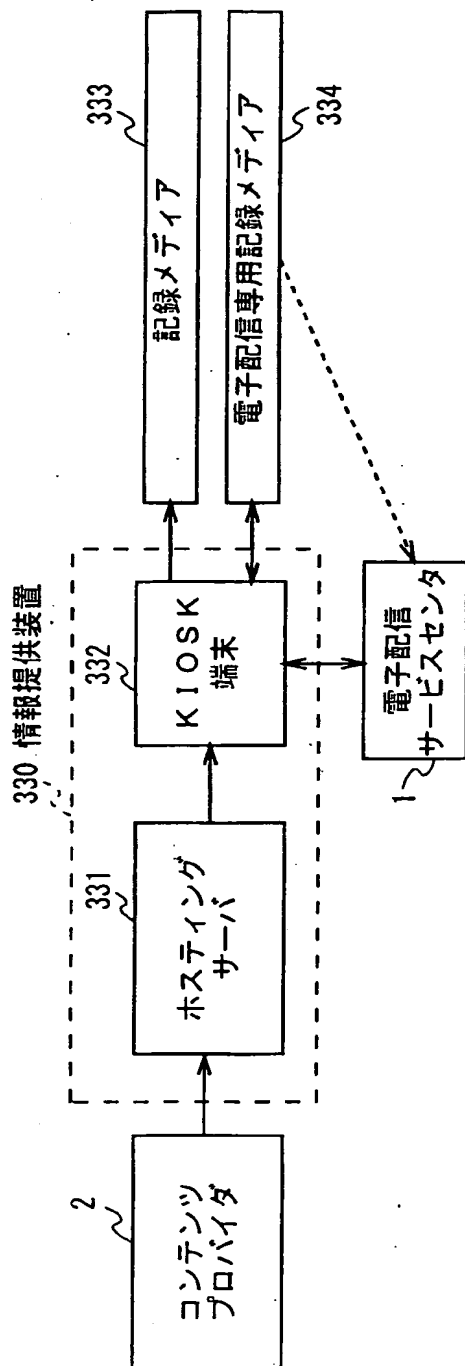


図 9 7





10

図 98

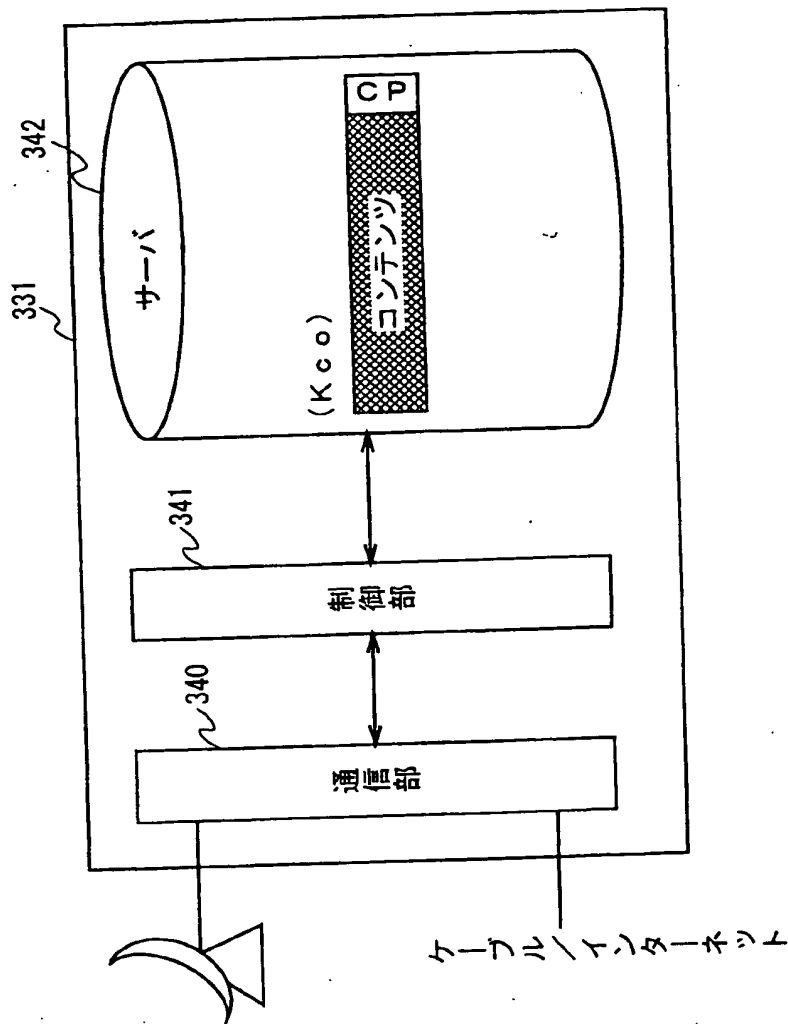


図 99

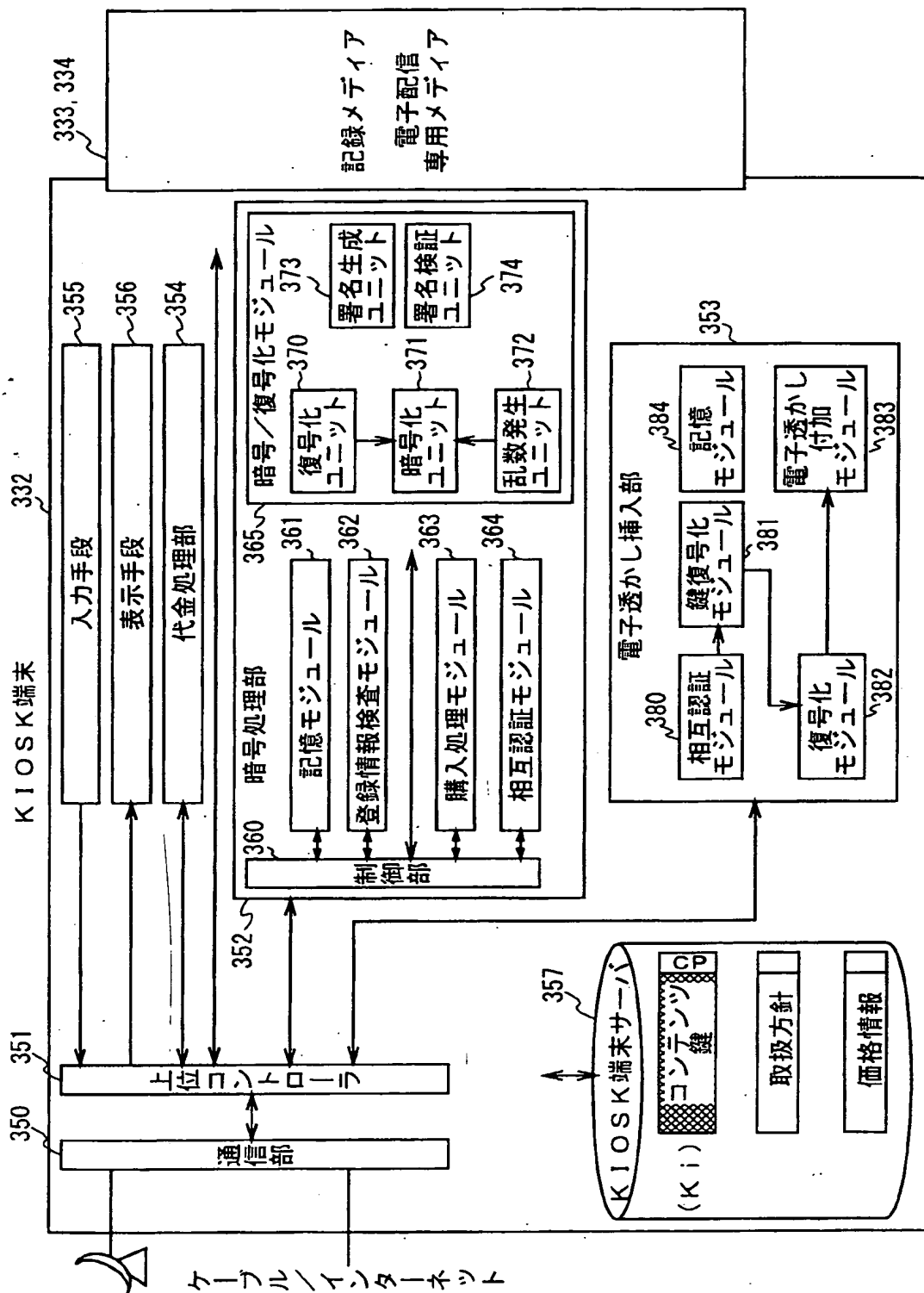


図 100

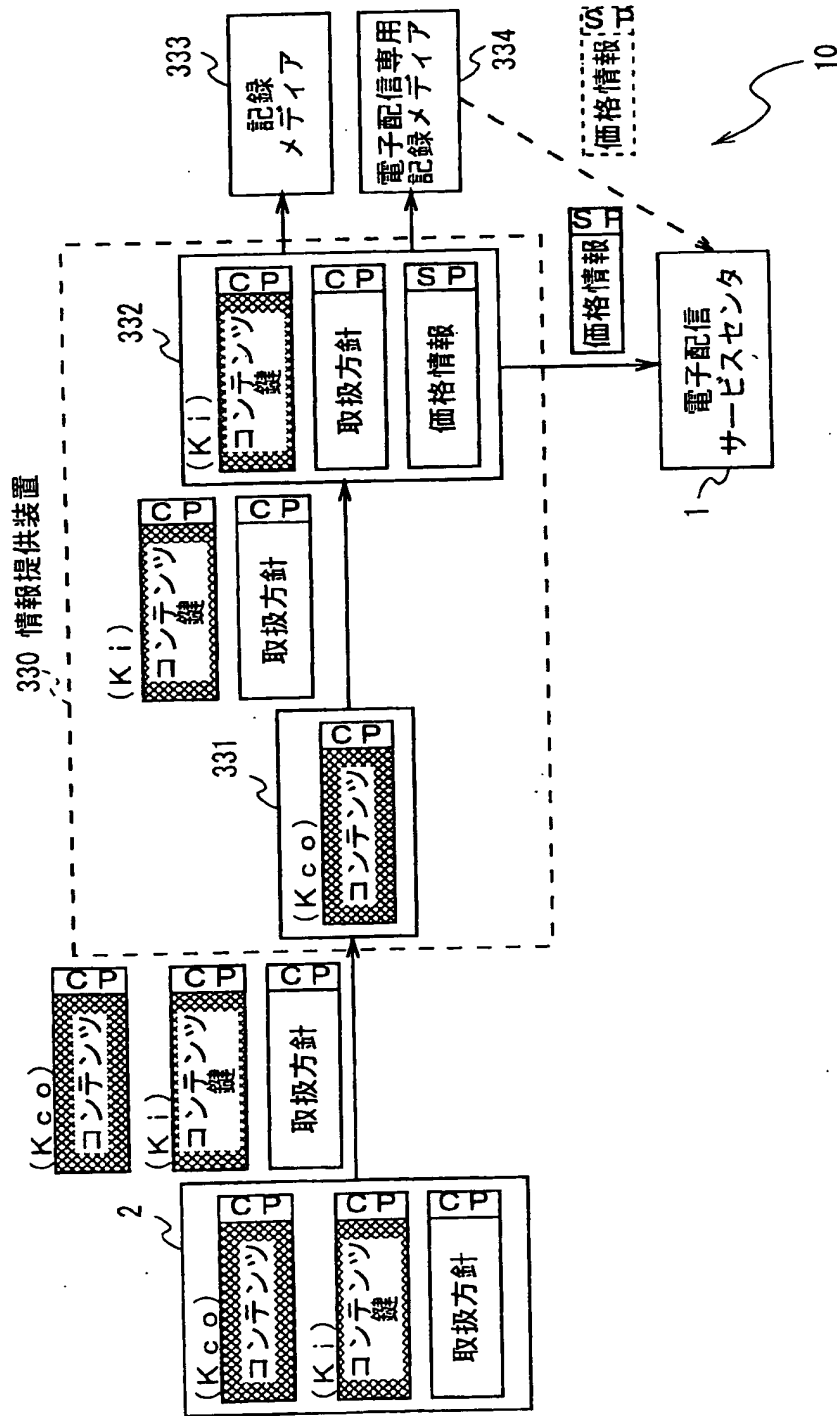


図101

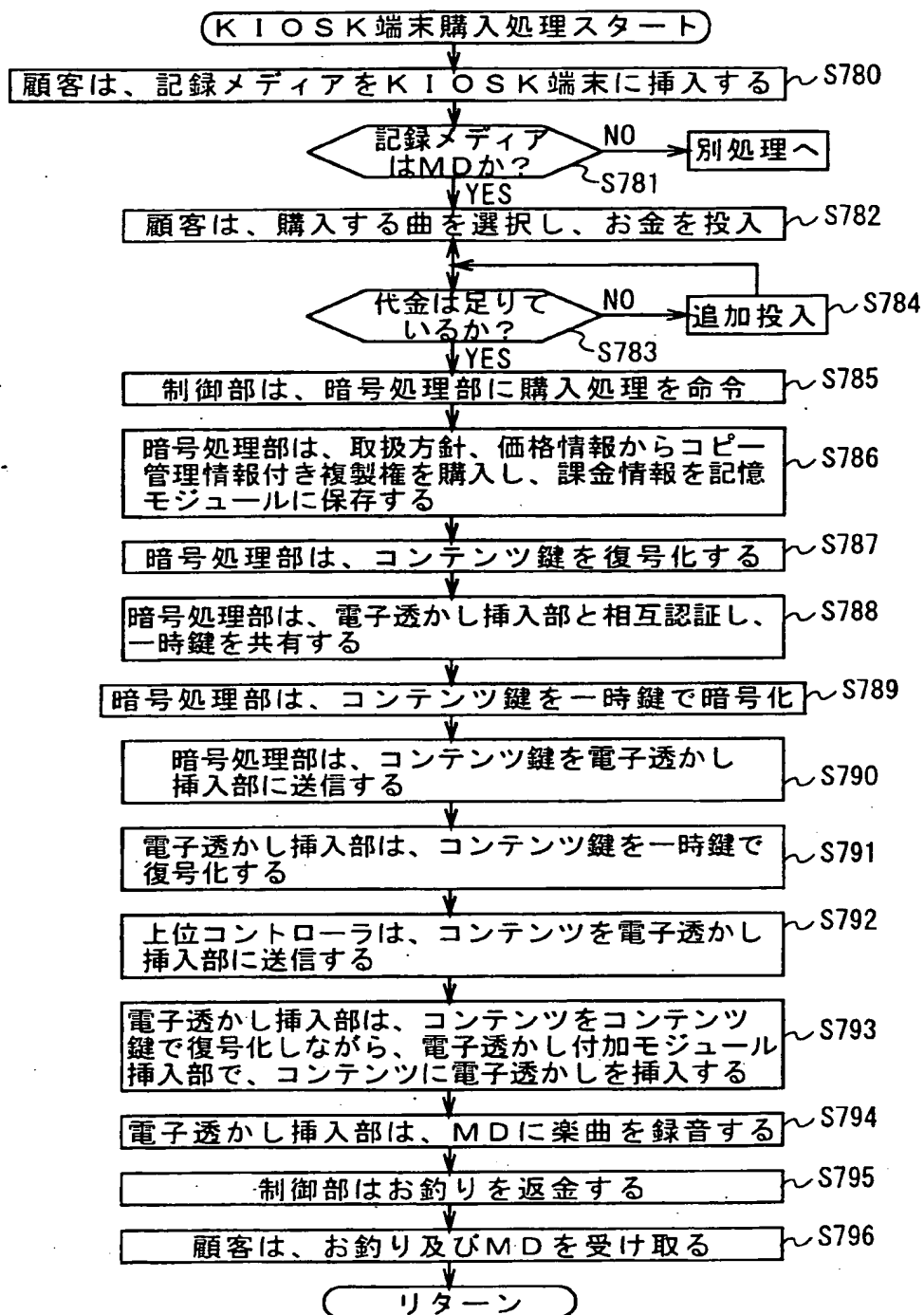


図 1 0 2

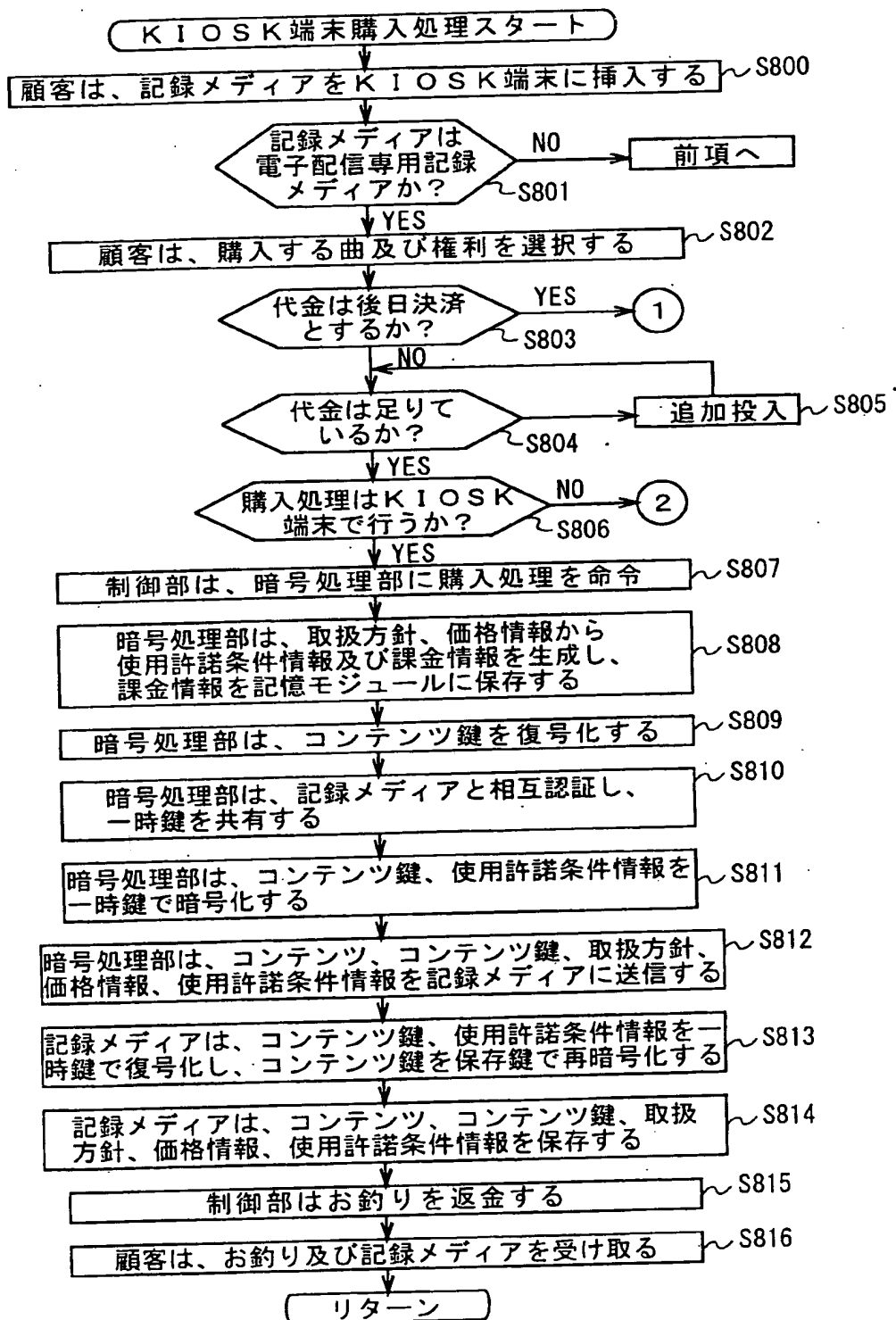


図 103

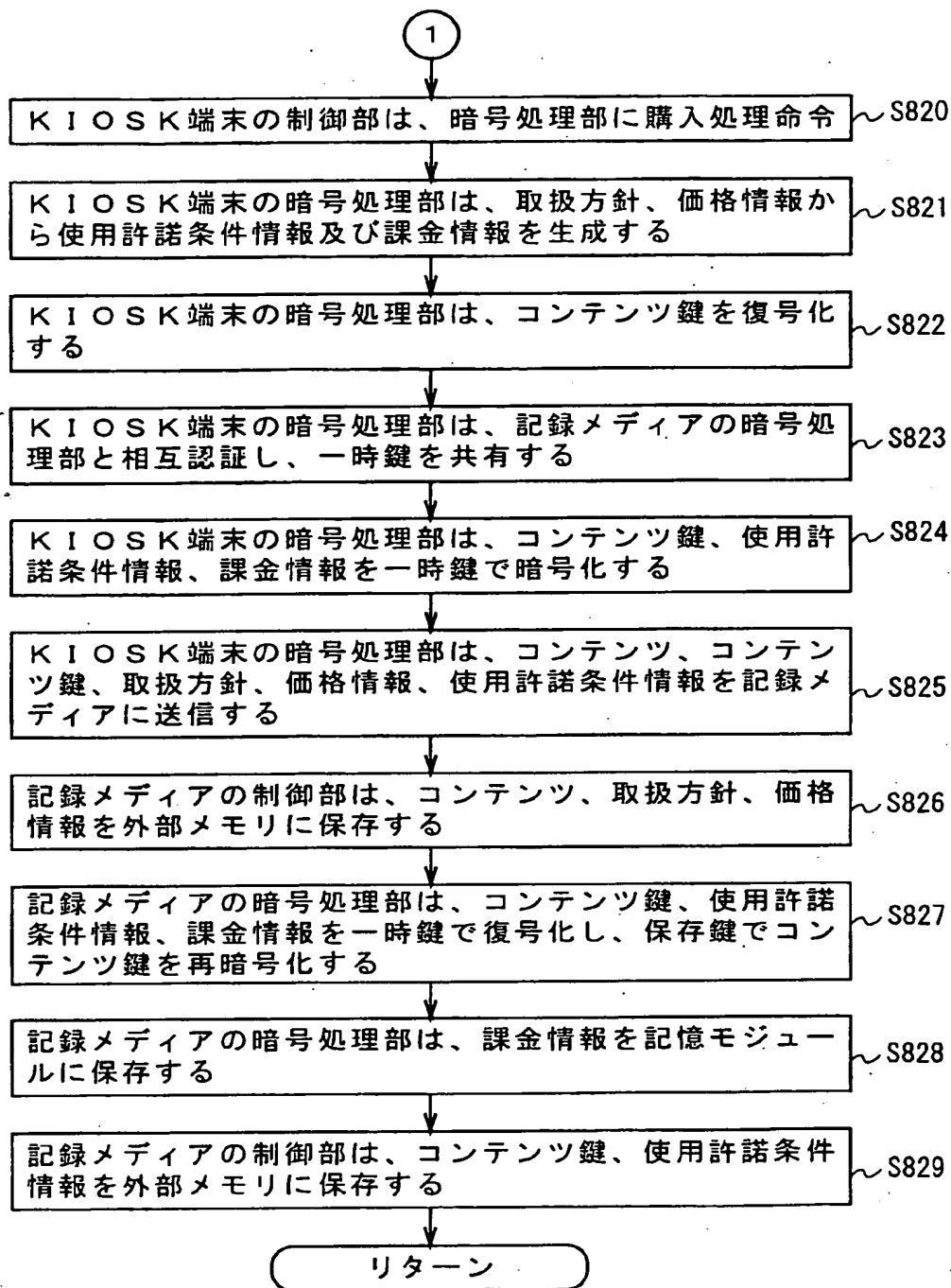
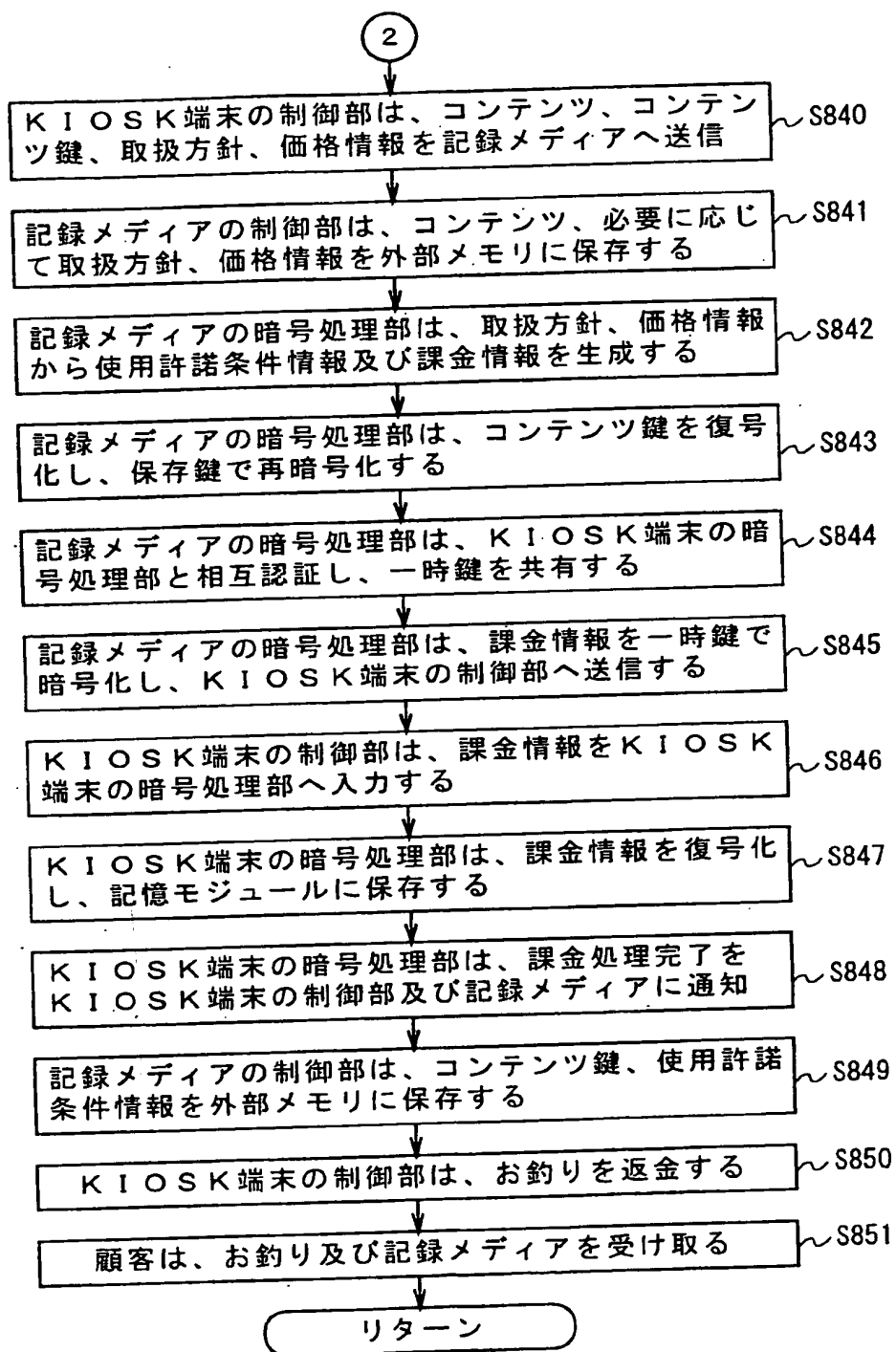


図 104





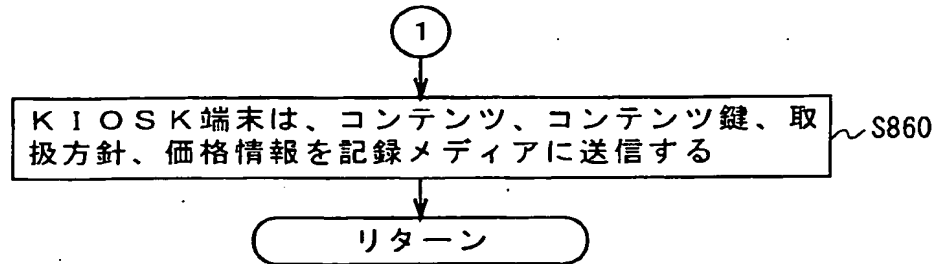


図 106

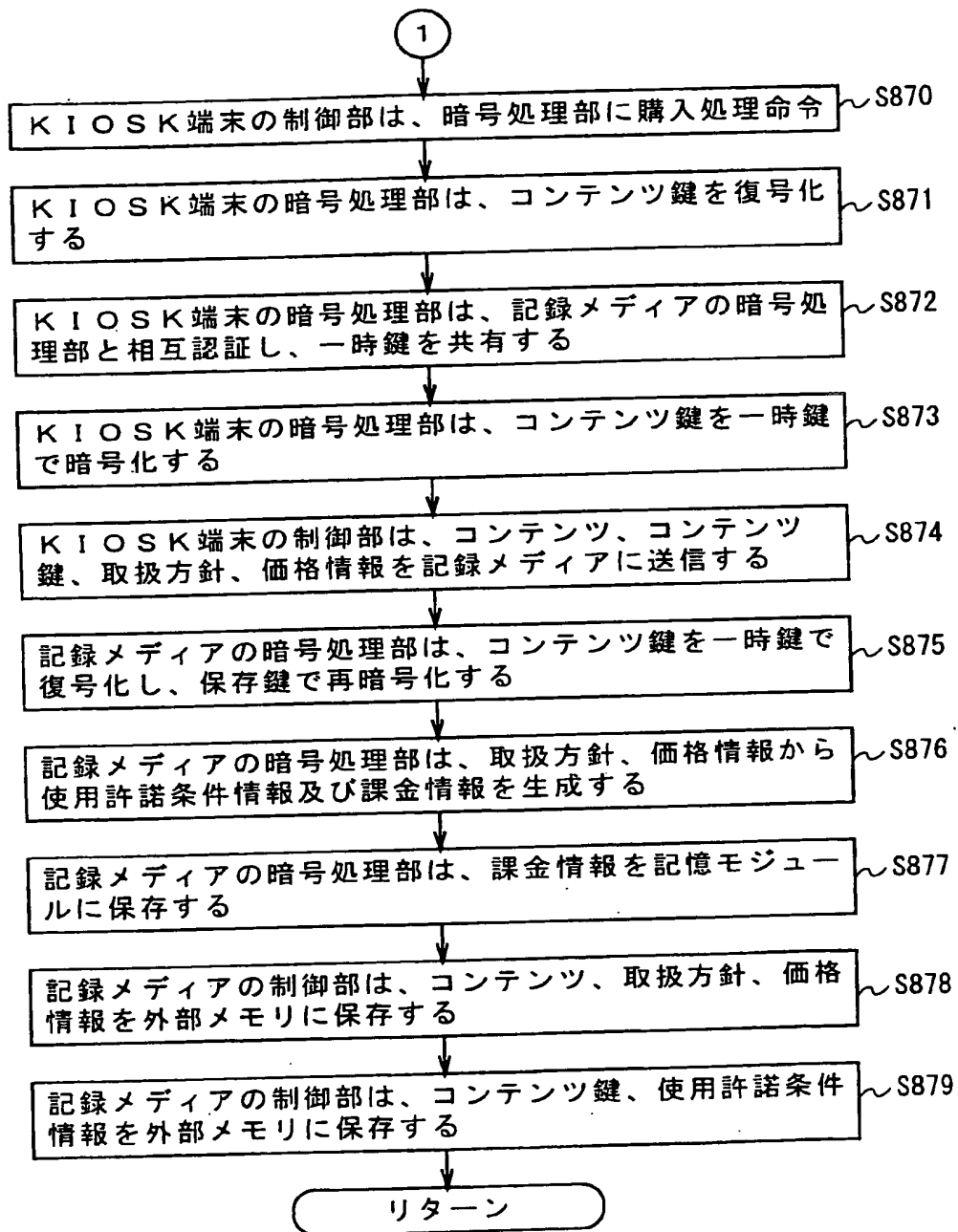


図 107

更新日付			
シリアル番号			
購入禁止 対象コンテンツ	コンテンツのID1	コンテンツのID2	...
	•	•	
	•	•	
	•	•	
利用禁止 対象コンテンツ プロバイダ	コンテンツプロバイダのID1	コンテンツプロバイダのID2	...
	•	•	
	•	•	
	•	•	
利用禁止 対象サービス プロバイダ	サービスプロバイダのID1	サービスプロバイダのID2	...
	•	•	
	•	•	
	•	•	
署名			

図 108

コンテンツのID1／コンテンツID1のID1／サブID1のID1／再配布／再購入先の暗号処理部のID1
コンテンツのID2／コンテンツID2のID2／サブID2のID2／再配布／再購入先の暗号処理部のID2
•
•
•
コンテンツのIDN／コンテンツIDNのIDN／サブIDNのIDN／再配布／再購入先の暗号処理部のIDN
署名

図 109

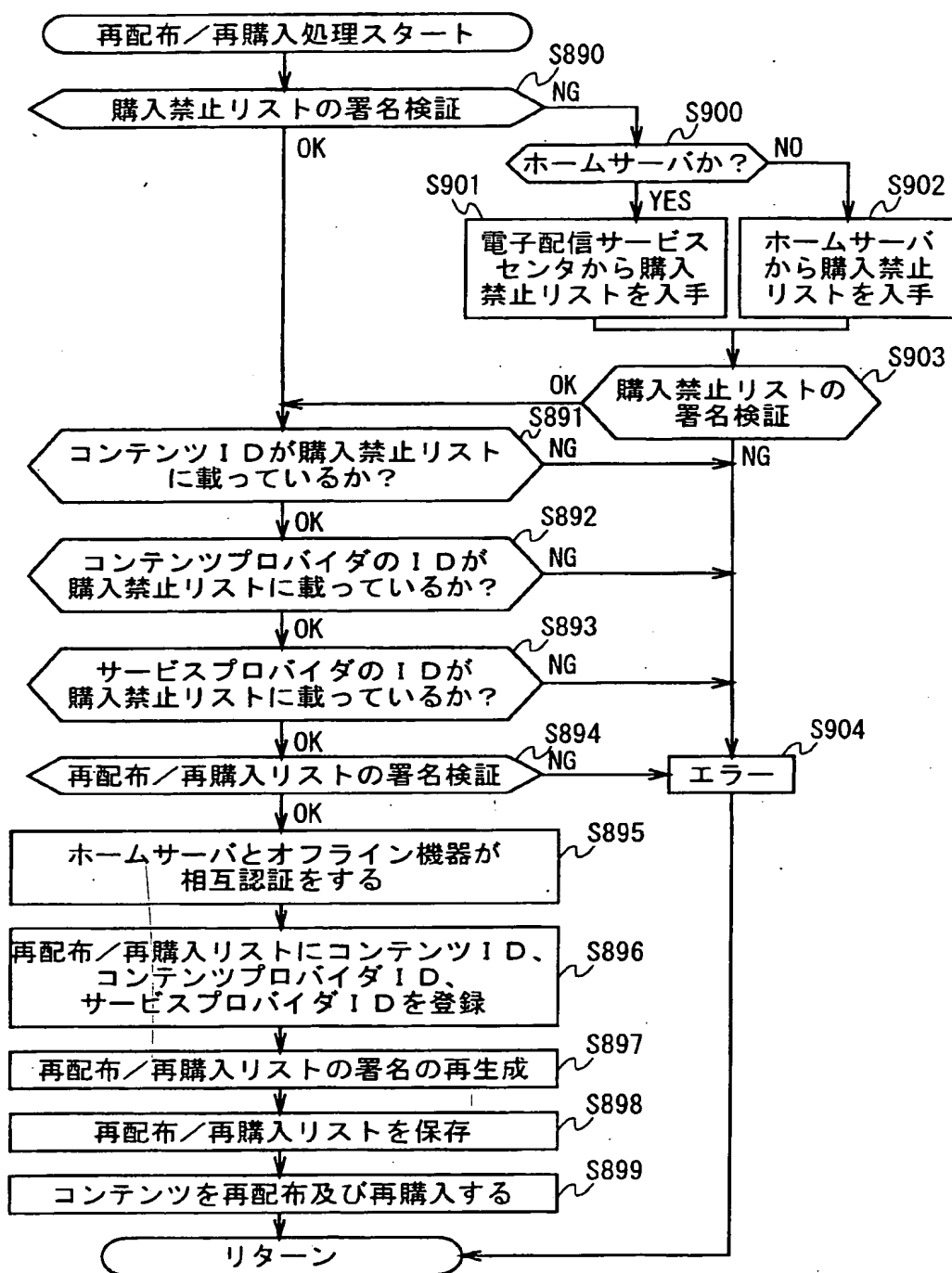


図 1 1 0

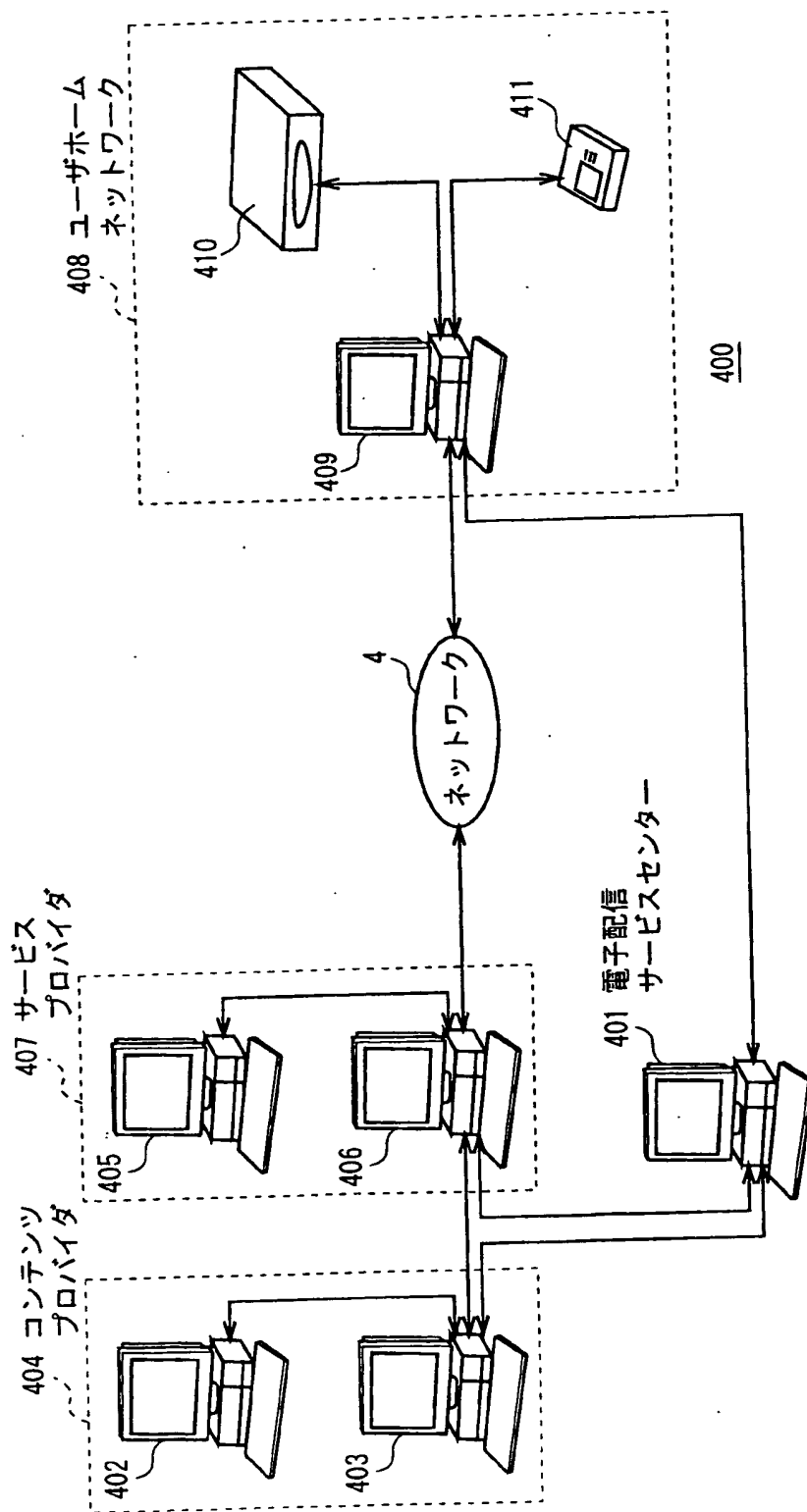


図 111

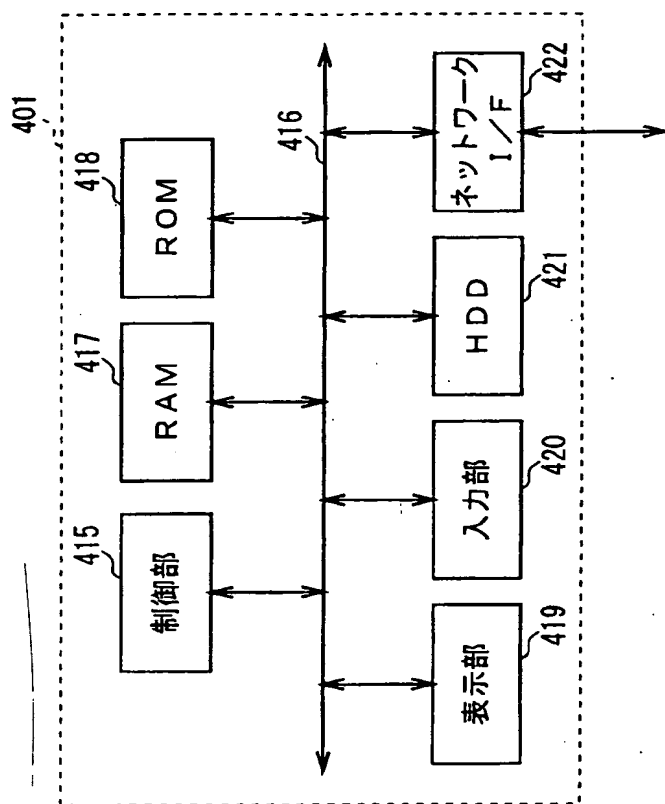


図 112

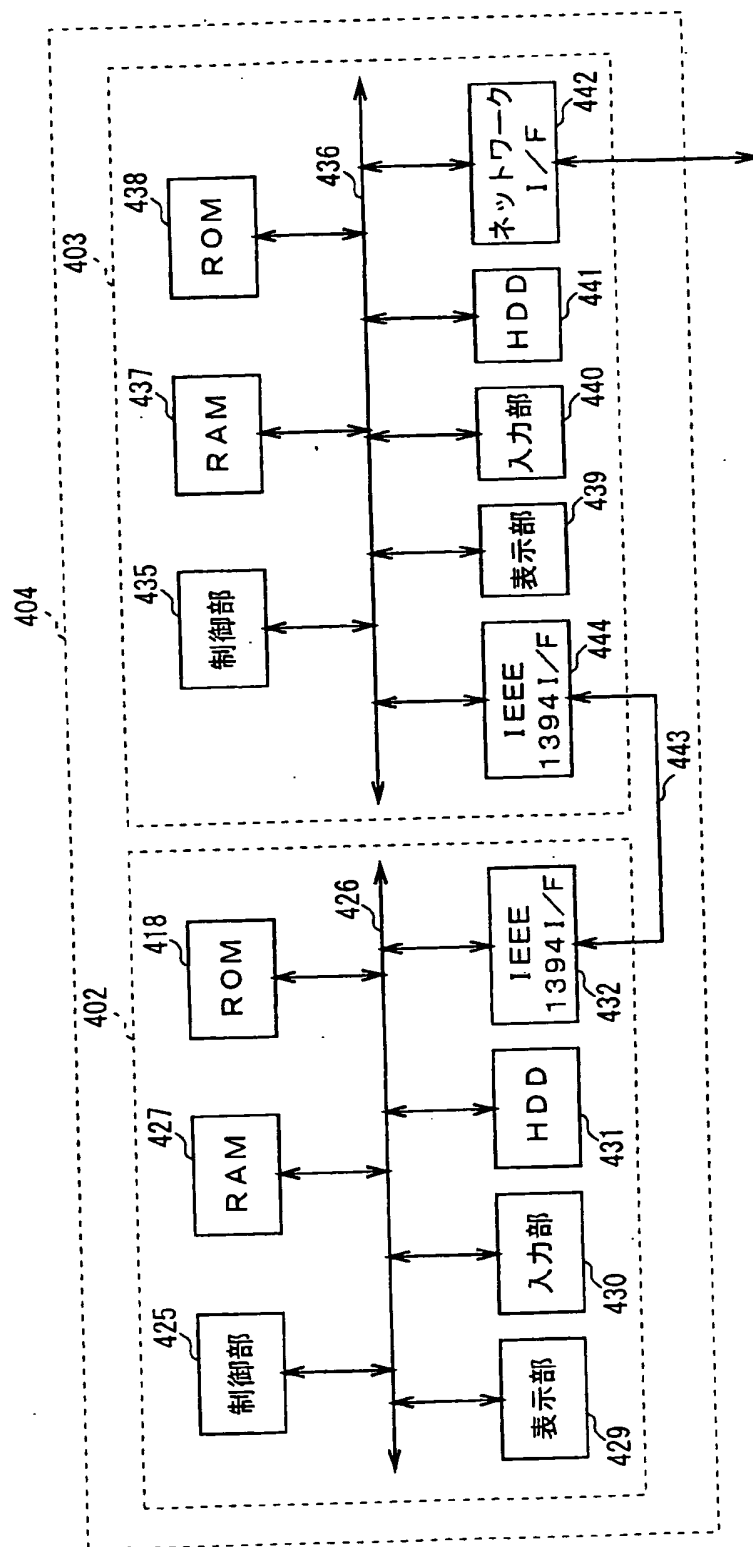


図 113



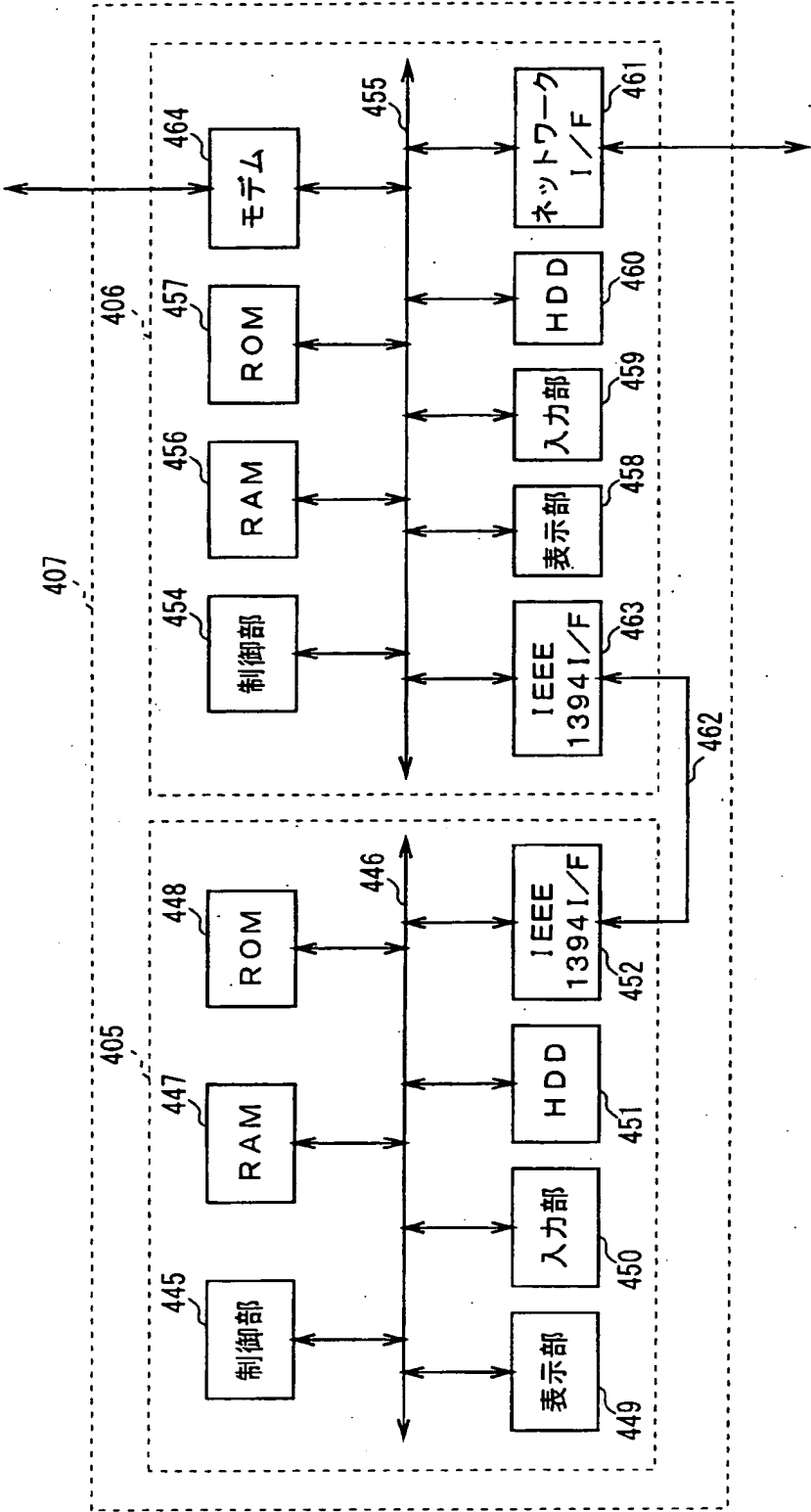


図 114

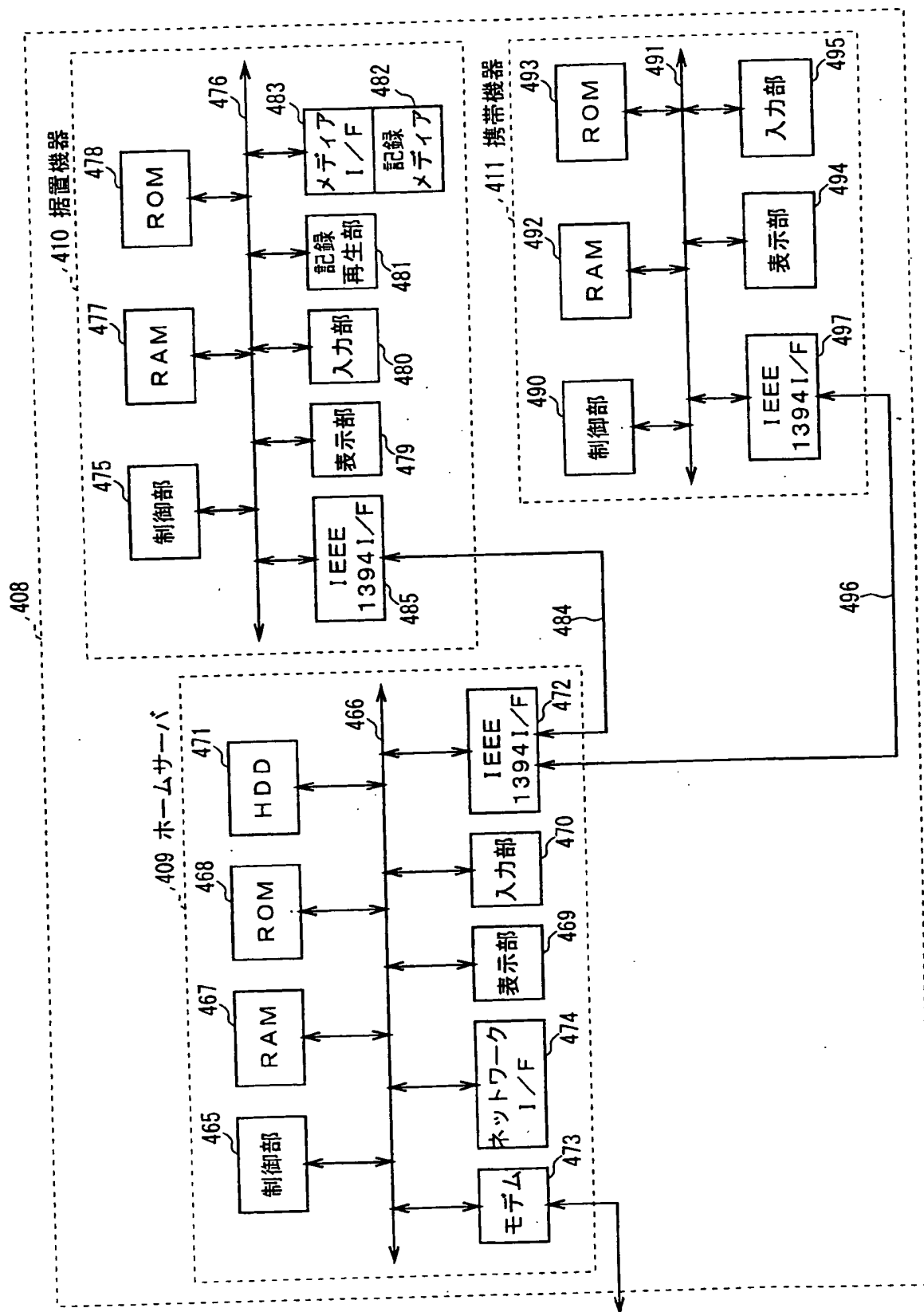


図 115

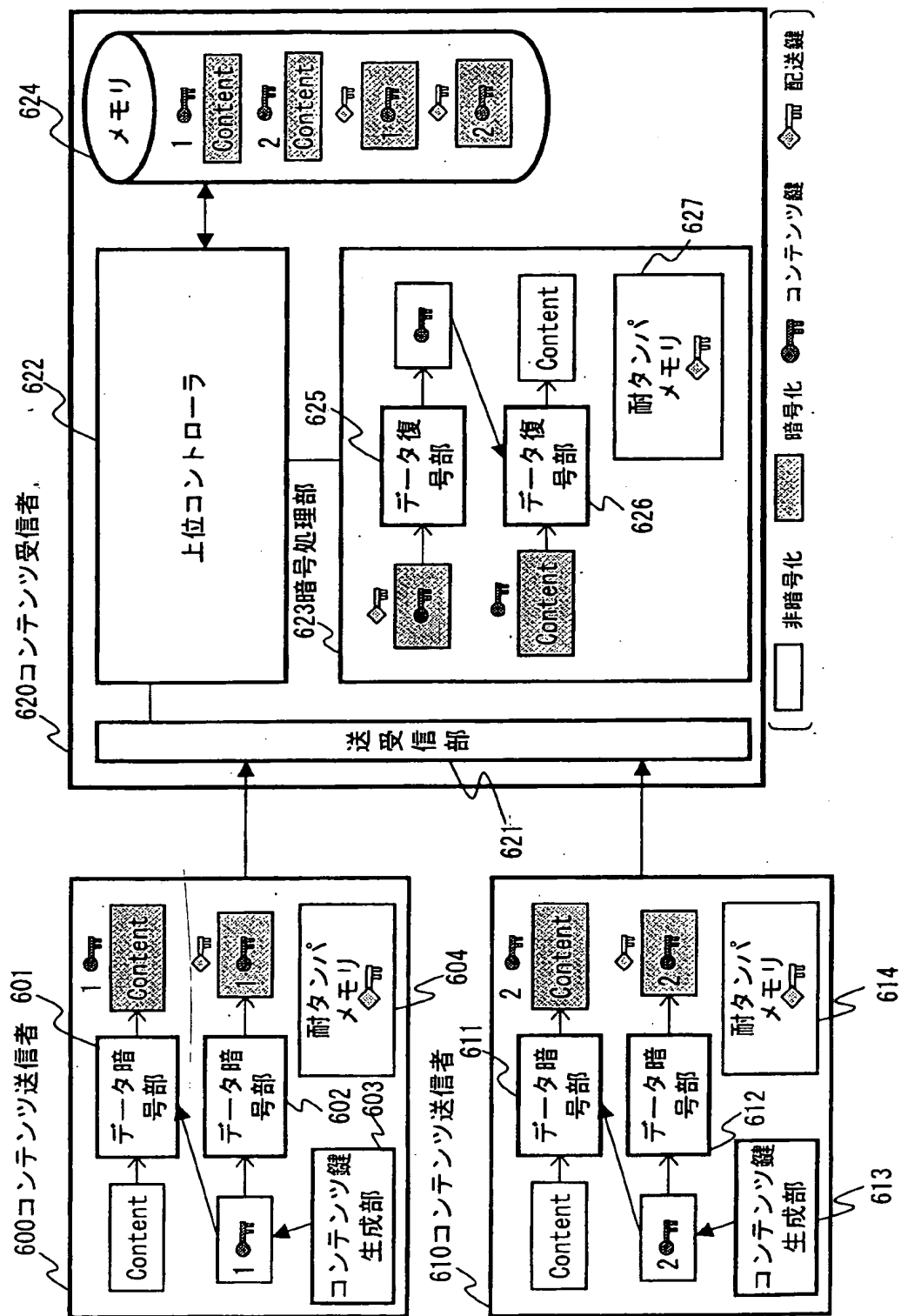


図116

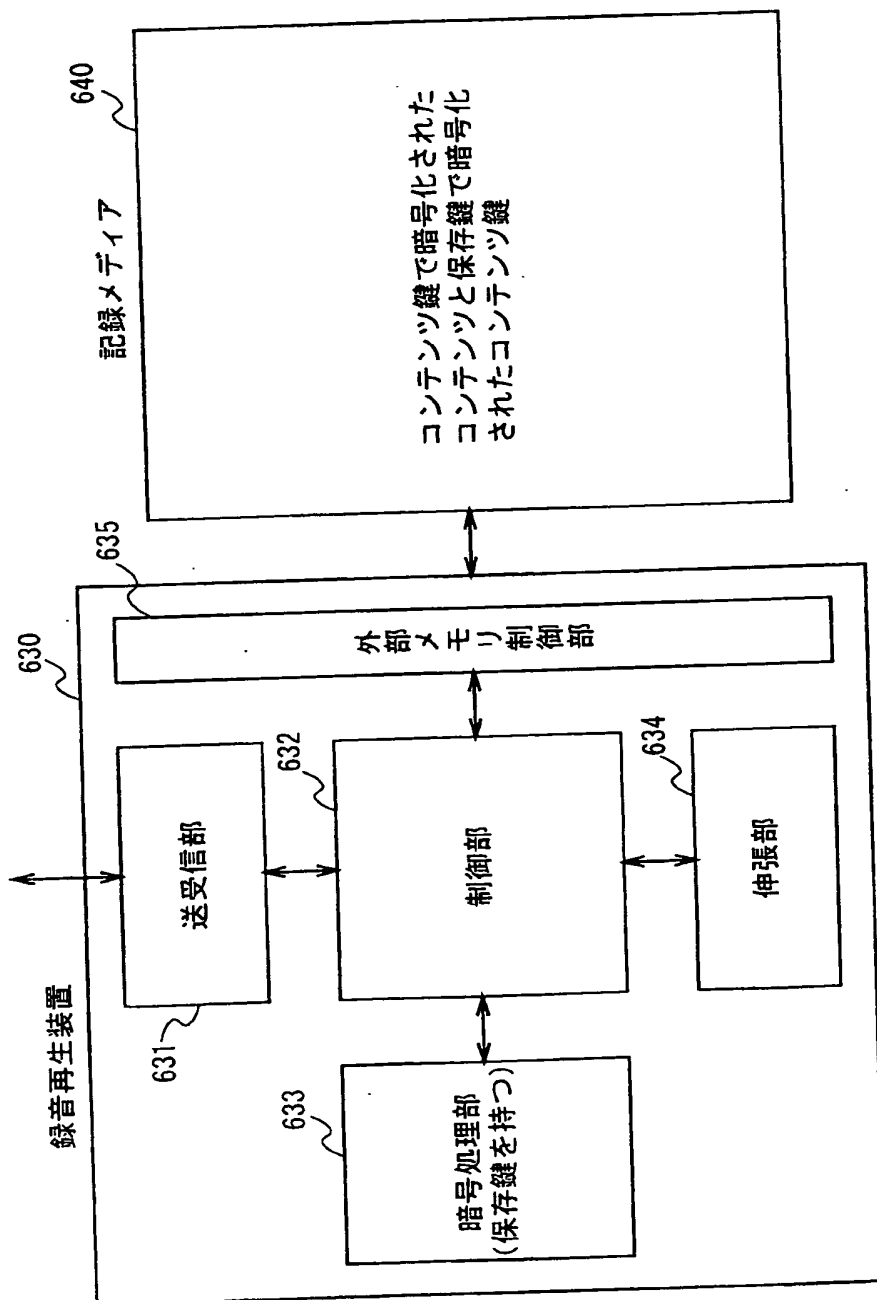


図 117

## 符 号 の 説 明

1、401……電子配信サービスセンタ、2、404……コンテンツプロバイダ、3、407……サービスプロバイダ、4……ネットワーク、5、408……ユーザホームネットワーク、10、400……電子音楽配信システム、34……コンテンツ暗号部、36……コンテンツ鍵暗号部、37、206……取扱方針生成部、38、45、207……署名生成部、40、202……メモリ、44……値付け部、51……ホームサーバ、61、260、300、350……通信部、62、351……上位コントローラ、65、122、262、301、352……暗号処理部、68……大容量記憶部、91、212、261、360……制御部、92、311……記憶モジュール、94……購入処理モジュール、96……暗号／復号化モジュール、111、320……復号化ユニット、115……署名検証ユニット、123、303……外部メモリ、130、302……外部メモリ制御部、203、204……データ暗号部、221……送受信部、222……署名検証部、223……データ復号部、226……比較器、250……記録再生装置、251、334……電子配信専用記録メディア、263……伸張部、321……暗号化ユニット、330……情報提供装置、331……ホスティングサーバ、332……KIOSK端末、333……記録メディア、353……電子透かし挿入部、402、405……サーバ用パーソナルコンピュータ、403、406……信号処理用パーソナルコンピュータ。

# INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP00/06089

A. CLASSIFICATION OF SUBJECT MATTER  
Int.Cl<sup>7</sup> H04L 9/32 G06F 15/00, H04N 5/91 G11B 20/10 G10K 15/04,  
H04N 7/167

According to International Patent Classification (IPC) or to both national classification and IPC

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)  
Int.Cl<sup>7</sup> G06F 15/00 G09C 1/00-5/00 G10K 15/00 G11B 20/10 H04H 1/00  
H04L 9/00 H04N 5/00-7/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)  
JICST FILE (JOIS)  
INSPEC (DIALOG)  
WPI (DIALOG)

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP, 8-305662, A (Fujitsu Limited), 22 November, 1996 (22.11.96), especially, Fig. 9 and Par. No. [0085] & US, 5784464, A	1-104
A	JP, 8-185444, A (Fujitsu Limited), 16 July, 1996 (16.07.96) (Family: none)	1-104
X	WO, 99/09718, A1 (Sony Corporation), 25 February, 1999 (25.02.99), especially, Fig. 8	105, 107, 108, 11 0, 112, 113, 115, 116
Y	& EP, 933901, A	106, 109, 111, 11 4, 117
Y	Kineo Matsui, "Internet Saishin Technology: the 13rd Digital Contents no Chiteki Shoyuiken wo mamoru Denshi Sukashi", "INTERNET magazine, No.37, (1998), pp.352-355, especially, p.355, left column	106, 109, 111, 11 4, 117, 292-300, 305-313, 318-32 1
Y	Fumitada Takahashi, "Digital Shingou Shori: "Denshi Sukashi" ga Multimedia Jidai wo mamoru; Chosakuken Hogo Gijutsu no Yuuryoku Kouho; Chosakubutsu no Fusei Riyou	106, 109, 111, 11 4, 117, 292-300, 305-313, 318-32

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

\* Special categories of cited documents:  
"A" document defining the general state of the art which is not  
considered to be of particular relevance  
"E" earlier document but published on or after the international filing  
date  
"L" document which may throw doubts on priority claim(s) or which is  
cited to establish the publication date of another citation or other  
special reason (as specified)  
"O" document referring to an oral disclosure, use, exhibition or other  
means  
"P" document published prior to the international filing date but later  
than the priority date claimed

"T" later document published after the international filing date or  
priority date and not in conflict with the application but cited to  
understand the principle or theory underlying the invention  
"X" document of particular relevance; the claimed invention cannot be  
considered novel or cannot be considered to involve an inventive  
step when the document is taken alone  
"Y" document of particular relevance; the claimed invention cannot be  
considered to involve an inventive step when the document is  
combined with one or more other such documents, such  
combination being obvious to a person skilled in the art  
"&" document member of the same patent family

Date of the actual completion of the international search  
22 November, 2000 (22.11.00)

Date of mailing of the international search report  
05 December, 2000 (05.12.00)

Name and mailing address of the ISA/  
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

## INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP00/06089

## C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
	Boushi ni Myoushu ari: Denshi Sukashi de Copy wo Yokusei" Nikkei Electronics, No.683, (1997), pp.99-107, especially, see page 107, right column, note	1
Y	ASANO, "Technology ga Ippai; Digital Contents wo mamoru Digital Sukashi", ASCII, Vol.21, No.9, (1997), pp.210-215, especially, page 214, lower right column, to page 215, left column	106,109,111,11 4,117,292-300, 305-313,318-32 1
X	Taro YOSHIO, "Kogata Memory Card de Ongaku Chosakuken wo mamoru", Nikkei Electronics, No.739, (22 March, 1999), pp.49-53	202,216,223, 237 118-201,203-21 5,217-222,224- 236,238-250,32 6,332-336,342- 346,352-355
Y	JP, 2-41051, A (Matsushita Electric Ind. Co., Ltd.), 09 February, 1990 (09.02.90) (Family: none)	118-194
Y	Fumitada TAKAHASHI, Taro YOSHIO, "Ongaku Haishin mattanashi; Seibi Isogu Chosakuken Hogo Gijutsu sasaeru Gijutsu Jitsuyouki no Haishin System; Chosakuken Kanri ga Kagi nigiru", Nikkei Electronics, No.738, (08, March, 1999), pp.94-98	120-122,126-12 8,132-134,138- 140,144-146,15 0-152,156-157, 163-165,169-17 1,175-177,181- 183,186-188, 191-193 356-395
A		
X	Tetsuo NAKAGAWA, et al., "Digital Contents Ryuutsu Gijutsu", Mitsubishi Denki Gihou, Vol.72, No.5 (1998), pp.36-39, especially, see chapter 4	196-201,203,21 5,217-222,224- 236,238-250,29 2-325,328-331, 333-335,338-34 1,343-345,348- 351,353-355
Y		
X	Shoko MOTOIKE, Masaki KIYONO, "DVD wo mochiita Contents Ryuutsu Service", Matsushita Technical Journal, Vol.44, No.5 (1998), pp.25-33, especially, see chapter 3	251-291 199-201,212-11 4,220-222,233- 236,247-250,29 2-325
Y	Naoji USUKI, et al., "5C Digital transmission Content Protection; IEEE1394 Bus no Chosakuken Hogo Houshiki", Eizou Media Gakkai Gijutsu Houkoku, Vol.22, No.65 (1998), pp.37-42 (CE'98-14)	200,201,207,20 8,214,215,221, 222,228,229,23 5,236,242,243, 249,250
Y	JP, 11-185381, A (Shoichi IIDA), 09 July, 1999 (09.07.99),	326,332-336,34 2-346,352-355
A	& WO, 99/21186, A1 & US, 5900608, A & AU, 8649198, A	327-331,337-34 1,347-351
Y	Daisuke IMAIZUMI, "Ongaku Haishin Souchi to shiten Internet", Computopia, Vol.34, No.393 (01 June, 1999), pp.96-97	326,332-336,34 2-346,352-355 327-331,337-34 1,347-351
A		

# INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP00/06089

## C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP, 7-182837, A (Hitachi Ltd.), 21 July, 1995 (21.07.05) (Family: none)	327-331, 337-34 1,347-351
X	Digital Transmission Content Protection Specification, Revision 1.0, (12 April, 1999), Informational Version	379,382,390, 393
A		1-378,380,381, 383-389,391,39 2,394,395
A	WO, 96/27155, A3 (Electronic Publishing Resources, Inc.), 06 September, 1996 (06.09.96), & JP, 10-512074, A & AU, 9663266, A & EP, 861461, A2 & US, 5910987, A & US, 5915019, A & US, 5917912, A & US, 5949876, A & US, 5982891, A	1-395
PY	Hironobu YAMAMOTO, et al., "Chosakuken wo Hogo shita Ongaku Haishin Platform", NTT R&D, Vol.48, No.10 (10 October, 1999), pp.762-769	1-355,379,382, 390,393, 356-378,380,38 1,383-389,391, 392,394,395
PA		



# INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP00/06089

## Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:  
because they relate to subject matter not required to be searched by this Authority, namely:
2. ☐ Claims Nos.:  
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:
3. ☐ Claims Nos.:  
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

## Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

The inventions of the international application are divided into ten groups.

1. The inventions of claims 1 to 104
2. The inventions of claims 105 to 117
3. The inventions of claims 118 to 194
4. The inventions of claims 195 to 208, 216 to 229, 237 to 243
5. The inventions of claims 209 to 215, 230 to 236, 244 to 250, 301 to 304, 314 to 317, 322 to 325
6. The inventions of claims 251 to 291
7. The inventions of claims 292 to 300, 305 to 313, 318 to 321
8. The inventions of claims 326 to 355
9. The inventions of claims 356 to 378, 385 to 389
10. The inventions of claims 379 to 384, 390 to 395

1. ☒ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.
2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.
3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:
4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest ☐ The additional search fees were accompanied by the applicant's protest.  
☒ No protest accompanied the payment of additional search fees.

## 国際調査報告

国際出願番号 PCT/JPO0/06089

## A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. Cl.<sup>7</sup>  
H04L 9/32 G06F 15/00, H04N 5/91 G11B 20/10 G10K 15/04, H04N 7/167

## B. 調査を行った分野

## 調査を行った最小限資料 (国際特許分類 (IPC))

Int. Cl.<sup>7</sup>  
G06F 15/00 G09C 1/00-5/00 G10K 15/00 G11B 20/10 H04H 1/00 H04L 9/00 H04N 5/00-7/00

最小限資料以外の資料で調査を行った分野に含まれるもの

## 国際調査で使用了電子データベース (データベースの名称、調査に使用した用語)

JICSTファイル (JOIS)  
INSPEC (DIALOG)  
WPI (DIALOG)

## C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
A	J P, 8-305662, A (富士通株式会社) 22. 11月. 1996 (22. 11. 96), 特に図9と第0085段落を参照 &US, 5784464, A	1-104
A	J P, 8-185444, A (富士通株式会社) 16. 7月. 1996 (16. 07. 96), (ファミリーなし)	1-104

☒ C欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

## \* 引用文献のカテゴリー

- 「A」 特に関連のある文献ではなく、一般的技術水準を示すもの  
「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの  
「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)  
「O」 口頭による開示、使用、展示等に言及する文献  
「P」 国際出願日前で、かつ優先権の主張の基礎となる出願

- の日の後に公表された文献  
「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの  
「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの  
「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの  
「&」 同一パテントファミリー文献

国際調査を完了した日 22. 11. 00

国際調査報告の発送日 05.12.00

国際調査機関の名称及びあて先  
日本国特許庁 (ISA/J P)  
郵便番号 100-8915  
東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)  
丸山 高政



5W 9570

電話番号 03-3581-1101 内線 3576

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
X	WO, 99/09718, A1 (ソニー株式会社) 25. 2月. 1999 (25. 02. 99), 特に第8図参照	105, 107, 108, 110, 112, 113, 115, 116
Y	&EP, 933901, A	106, 109, 111, 114, 117
Y	松井 甲子雄 “インターネット最新テクノロジー：第13回 デジタルコンテンツの知的所有権を守る電子透かし” INTERNET magazine, No. 37, (1998), pp. 352-355, 特に355頁左欄参照	106, 109, 111, 114, 117, 292- 300, 305-313, 318-321
Y	高橋 史忠 “ディジタル信号処理：「電子透かし」がマルチメディ ア時代を守る 著作権保護技術の有力候補 著作物の不正利用防止 に妙手あり、電子透かしでコピーを抑制” 日経エレクトロニクス, No. 683, (1997), pp. 99-107, 特に107頁右欄ただし書き参照	106, 109, 111, 114, 117, 292- 300, 305-313, 318-321
Y	浅野 “テクノロジーがいっぱい デジタルコンテンツを守るデジタル透かし” ASCI I, Vol. 21, No. 9, (1997), pp. 210-215, 特に214頁右欄下から215頁左欄参照	106, 109, 111, 114, 117, 292- 300, 305-313, 318-321
X	芳尾 太郎 “小型メモリ・カードで音楽著作権を守る” 日経エレクトロニクス, No. 739, (1999年3月22日), pp. 49-53	202, 216, 223, 237
Y		118-201, 203- 215, 217-222, 224-236, 238- 250, 326, 332- 336, 342-346, 352-355
Y	JP, 2-41051, A (松下電器産業株式会社) 9. 2月. 1990 (09. 02. 90), ファミリーなし	118-194
Y	高橋 史忠, 芳尾 太郎 “音楽配信マッタナシ・整備急ぐ著作権保護 技術 支える技術 実用期の配信システム、著作権管理がカギ握る” 日経エレクトロニクス, No. 738, (1999年3月8日), pp. 94-98	120-122, 126- 128, 132-134, 138-140, 144- 146, 150-152, 156-157, 163- 165, 169-171, 175-177, 181- 183, 186-188, 191-193 356-395
A		

C (続き). 関連すると認められる文献		関連する 請求の範囲の番号
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	
Y	中川路 哲男, 石塚 裕一, 宮崎 一哉, 中嶋 春光 “デジタルコンテンツ流通技術” 三菱電機技法, Vol. 72. No. 5, (1998), pp. 36-39 特に第4章参照	196-201, 203- 215, 217-222, 224-236, 238- 250, 292-325, 328-331, 333- 335, 338-341, 343-345, 348- 351, 353-355
X Y	本池 祥子, 清野 正樹 “DVDを用いたコンテンツ流通サービス” Matsushita Technical Journal, Vol. 44, No. 5, (1998), pp. 25-33 特に第3章参照	251-291 199-201, 212- 114, 220-222, 233-236, 247- 250, 292-325
Y	臼木 直司, 飯塚 裕之, 山田 正純, 松崎 なつめ “5C Digital Transmission Content Protection IEEE1394バスの著作権保護方式” 映像メディア学会技術報告, Vol. 22, No. 65, (1998), pp. 37-42 (CE' 98-14)	200, 201, 207, 208, 214, 215, 221, 222, 228, 229, 235, 236, 242, 243, 249, 250
Y A	JP, 11-185381, A (飯田 尚一) 9. 7月. 1999 (09. 07. 99) &WO, 99/21186, A1 &US, 5900608, A &AU, 8649198, A	326, 332-336, 342-346, 352- 355 327-331, 337- 341, 347-351
Y A	今泉 大輔 “音楽配信装置としてのインターネット” Computopia, Vol. 34, No. 393, (1999年6月1日), pp. 96-97	326, 332-336, 342-346, 352- 355 327-331, 337- 341, 347-351
A	JP, 7-182837, A (株式会社日立製作所) 21. 7月. 1995 (21. 07. 95), ファミリーなし	327-331, 337- 341, 347-351

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
X	Digital Transmission Content Protection Specification, Revision 1.0, (1999 April 12), Informational Version	379, 382, 390, 393
A		1-378, 380, 381, 383-389, 391, 392, 394, 395
A	WO, 96/27155, A3 (Electronic Publishing Resources, Inc.) 6. 9月. 1996 (06. 09. 96) & JP, 10-512074, A & AU, 9663266, A & EP, 861461, A2 & US, 5910987, A & US, 5915019, A & US, 5917912, A & US, 5949876, A & US, 5982891, A	1-395
PY	山本 博伸, 荒木 秀教, 野村 進, 山下 康博, 浅野 真樹 “著作権を保護した音楽配信プラットフォーム”	1-355, 379, 382, 390, 393
PA	NTT R&D, Vol. 48, No. 10, (1999年10月10日), pp. 762-769	356-378, 380, 381, 383-389, 391, 392, 394, 395

## 第Ⅰ欄 請求の範囲の一部の調査ができないときの意見 (第1ページの2の続き)

法第8条第3項 (PCT17条(2)(a)) の規定により、この国際調査報告は次の理由により請求の範囲の一部について作成しなかった。

1. ☐ 請求の範囲 \_\_\_\_\_ は、この国際調査機関が調査をすることを要しない対象に係るものである。  
つまり、
2. ☐ 請求の範囲 \_\_\_\_\_ は、有意義な国際調査をすることができる程度まで所定の要件を満たしていない国際出願の部分に係るものである。つまり、
3. ☐ 請求の範囲 \_\_\_\_\_ は、従属請求の範囲であってPCT規則6.4(a)の第2文及び第3文の規定に従って記載されていない。

## 第Ⅱ欄 発明の単一性が欠如しているときの意見 (第1ページの3の続き)

次に述べるようにこの国際出願に二以上の発明があるとこの国際調査機関は認めた。

この出願の発明は、以下の10群の発明に区分される。

- |  |                                   |
|--|-----------------------------------|
| 1. 請求の範囲1-104  | 6. 請求の範囲251-291                   |
| 2. 請求の範囲105-117  | 7. 請求の範囲292-300, 305-313, 318-321 |
| 3. 請求の範囲118-194  | 8. 請求の範囲326-355                   |
| 4. 請求の範囲195-208, 216-229, 237-243                            | 9. 請求の範囲356-378, 385-389          |
| 5. 請求の範囲209-215, 230-236, 244-250, 301-304, 314-317, 322-325 | 10. 請求の範囲379-384, 390-395         |

1. ☒ 出願人が必要な追加調査手数料をすべて期間内に納付したので、この国際調査報告は、すべての調査可能な請求の範囲について作成した。
2. ☐ 追加調査手数料を要求するまでもなく、すべての調査可能な請求の範囲について調査することができたので、追加調査手数料の納付を求めなかった。
3. ☐ 出願人が必要な追加調査手数料を \_\_\_\_\_ のみしか期間内に納付しなかったので、この国際調査報告は、手数料の納付のあった次の請求の範囲のみについて作成した。
4. ☐ 出願人が必要な追加調査手数料を期間内に納付しなかったので、この国際調査報告は、請求の範囲の最初に記載されている発明に係る次の請求の範囲について作成した。

追加調査手数料の異議の中立てに関する注意

- ☐ 追加調査手数料の納付と共に出願人から異議申立てがあった。
- ☒ 追加調査手数料の納付と共に出願人から異議申立てがなかった。

**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

**BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☒ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☒ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☒ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**

**THIS PAGE BLANK (USPTO)**